Gericht

BVwG

Entscheidungsdatum

21.10.2014

Geschäftszahl

W134 2010888-1

Spruch

W134 2000196-1/25E

W134 2003810-1/22E

W134 2006715-1/11E

W134 2006716-1/11E

W134 2010887-1/11E

W134 2010888-1/11E

BESCHLUSS

Das Bundesverwaltungsgericht hat durch den Richter Mag. Thomas Gruber als Einzelrichter über zwei zur gemeinsamen Verhandlung und Entscheidung verbundene Maßnahmenbeschwerden vom 30.09.2013 der XXXX, alle vertreten durch XXXX, betreffend zwei Hausdurchsuchungen nämlich vom 19.08.2013 bis 20.08.2013 in XXXX, und am 20.08.2013 in XXXX, gegen die Bundeswettbewerbsbehörde, Praterstraße 31, 1020 Wien, vertreten durch die XXXX, nach Durchführung einer mündlichen Verhandlung am 16.09.2014 beschlossen:

A)

I. Die Beschwerden werden gemäß Art 130 Abs. 1 Z 2 B-VG als unzulässig zurückgewiesen.

B)

Die Revision ist gemäß Art. 133 Abs. 4 B nicht zulässig.

Text

BEGRÜNDUNG:

I. Verfahrensgang:

Mit Hausdurchsuchungsbefehl vom 06.08.2013 ordnete das Oberlandesgericht Wien als Kartellgericht über Antrag der Bundeswettbewerbsbehörde (kurz "BWB" genannt) eine Hausdurchsuchung in den Geschäftsräumlichkeiten und Fahrzeugen der Erstbeschwerdeführerin am Standort XXXX, an und erweiterte diesen mit Beschluss vom 20.08.2013.

Mit Schreiben an den UVS Salzburg vom 30.09.2013 erhoben die Beschwerdeführerinnen eine Maßnahmenbeschwerde gegen die Hausdurchsuchung am 20.08.2013 in XXXX. Mit Schreiben an den UVS Kärnten vom 30.09.2013 erhoben die Beschwerdeführerinnen eine Maßnahmenbeschwerde gegen die

Hausdurchsuchung vom 19.08.2013 bis 20.08.2013 in XXXX, worin sie zum Sachverhalt und den Beschwerdegründen vorbringen (die Beweisanträge wurden weggelassen):

"4. Einschreitende BWB-Mitarbeiter

Der Behördenleiter der belangten Behörde, der Generaldirektor für Wettbewerb XXXX, hat am 16.08.2013 die im Rubrum angeführten Bediensteten der belangten Behörde berechtigt, im Namen der belangten Behörde die verfahrensgegenständliche Hausdurchsuchung aufgrund des Hausdurchsuchungsbefehls des OLG Wien vom 06.08.2013, 26 Kt 88/13-2, durchzuführen. Als Einsatzleiter fungierten Dr. XXXX und Mag. XXXX.

Entgegen der ausdrücklichen Anordnung gem § 12 Abs 3 letzter Satz WettbG wurde der Hausdurchsuchungsbefehl von der belangten Behörde jedoch nicht innerhalb von 24 Stunden zugestellt.

5. Beginn der Hausdurchsuchung am 19.08.2013

Am 19.08.2013 betraten gegen 10:10 Uhr Mitarbeiter der BWB gemeinsam mit zur Unterstützung beigezogenen Mitarbeitern des Bundeskriminalamtes (im Folgenden kurz als "BKA" bezeichnet) und weiteren uniformierten Polizisten als Hilfskräfte der BWB die Geschäftsräumlichkeiten der erstbeschwerdeführenden Partei in XXXX XXXX, und setzten den Hausdurchsuchungsbefehl vom 06.08.2013 in Vollzug. Mit Ausnahme der uniformierten Polizisten waren weder die Bediensteten der BWB noch die Beamten des BKA aufgrund ihrer Bekleidung als solche zu erkennen.

Gegenüber der am Empfang tätigen Mitarbeiterin von XXXX identifizierte sich die BWB ebenfalls nicht als solche. Es wurde lediglich behauptet, dass ein behördliches Schriftstück an die Geschäftsleitung der Zweigniederlassung zuzustellen sei. Nähere Informationen, um welche Entscheidung es sich konkret handelt, wurden nicht genannt. Es wurde von der belangten Behörde daher insbesondere verschwiegen, dass es sich um einen gerichtlichen Hausdurchsuchungsbefehl nach dem WettbG handelt. Eine Übergabe des - von der belangten Behörde nach wie vor nicht als solchen bezeichneten - Hausdurchsuchungsbefehls an die am Empfang tätige Mitarbeiterin von XXXX wurde mit der Begründung abgelehnt, dass dieses Dokument persönlich an den Geschäftsführer der Zweigniederlassung zu übergeben sei.

Die XXXX XXXX wird von den Prokuristen XXXX, XXXX und XXXX jeweils gemeinsam mit einem Vorstandmitglied oder einem zweiten auf dieselbe Zweigniederlassung beschränkten Gesamtprokuristen rechtsgeschäftlich vertreten. Den vorgenannten Prokuristen, insbesondere XXXX, kommt die operative Leitung der XXXX XXXX zu. Aufgrund dieses Umstandes und da XXXX auch als gewerberechtlicher Geschäftsführer für die XXXX XXXX fungiert, werden diese intern auch als "Geschäftsführer" tituliert, was handelsrechtlich aber nicht der Fall ist.

Es handelt sich sohin bei diesen Prokuristen um keine organschaftlichen Vertreter von XXXX. Da jedoch bereits im Jänner und Februar 2013 in der Hauptzentrale von XXXX in XXXX, eine Hausdurchsuchung durch die BWB stattgefunden hatte, wurden die jeweiligen Leiter der Zweigniederlassungen von XXXX bevollmächtigt und beauftragt, Befragungen gern § 12 Abs 5 WettbG zu beantworten. Diese Bevollmächtigung und Beauftragung umfasste insbesondere auch den Auftrag, die von der belangten Behörde im Rahmen einer gem § 12 Abs 5 WettbG vor einer angeordneten Hausdurchsuchung zwingend durchzuführenden Befragung zu bezeichneten Unterlagen herauszugeben.

Es ist daher bereits an dieser Stelle darauf hinzuweisen, dass die BWB bis zur Einvernahme von XXXX am 19.08.2013 gegen ca 17:50 Uhr davon ausging, dass es sich bei XXXX um einen Geschäftsführer bzw Vorstand und sohin einen organschaftlichen Vertreter von XXXX handeln würde (obwohl das Gegenteil aus dem offenen Firmenbuch bei angemessener Vorbereitung einfach ersichtlich gewesen wäre).

Da sich XXXX, dessen Büro direkt hinter dem Empfangsbereich situiert ist, im Zeitpunkt des Eintreffens der BWB in einer Besprechung befand, hat dessen persönliche Assistentin, XXXX, die Bediensteten der BWB, die nach wie vor nicht als solche erkennbar waren, darauf hingewiesen, dass XXXX derzeit nicht gestört werden könne. Die BWB hat jedoch darauf bestanden, dass XXXX erscheint, da ihm ein behördliches Schriftstück persönlich zuzustellen sei. Daraufhin hat XXXX die Besprechung, in der sich XXXX befand, unterbrochen und diesen ersucht, sich in den Empfangsbereich zu begeben.

Sämtliche Bediensteten der BWB, deren Hilfskräfte vom BKA sowie die uniformierten Polizisten wurden von XXXX persönlich mit Handschlag begrüßt. Auch zu diesem Zeitpunkt gaben sich die Bediensteten der BWB noch nicht als solche zu erkennen. XXXX hat sämtliche Bediensteten der BWB sowie deren Hilfskräfte

daraufhin in einen unmittelbar hinter dem Empfangsbereich befindlichen Besprechungsraum geführt. Erst dort identifizierten sich die Bediensteten der BWB und des BKA als solche. Daraufhin hat XXXX seine persönliche Assistentin gebeten, den weiteren Prokuristen XXXX sofort zu diesem Gespräch zu holen.

Nachdem auch XXXX zu dieser Runde gestoßen war, wurde XXXX der Hausdurchsuchungsbefehl - jedoch ohne jede weitere Erläuterungen, um welches Dokument es sich konkret handelt und insbesondere welcher Untersuchungsgegenstand darin definiert ist - übergeben; parallel wurde ein weiteres Exemplar XXXX vorgelegt.

Unmittelbar mit der Übergabe des Hausdurchsuchungsbefehls, also noch bevor überhaupt nur die erste Seite gelesen werden konnte, wurde seitens der belangten Behörde Auskunft verlangt, wo sich die Einkaufsabteilungen befinden. Zunächst wollte XXXX diese Frage nicht beantworten, da er zuvor den Hausdurchsuchungsbefehl durchlesen wollte. Da jedoch seitens der BWB ein enormer Druck aufgebaut wurde, die Büroräumlichkeiten zu betreten, begaben sich die Bediensteten der belangten Behörde sowie deren Hilfskräfte ohne unsere Zustimmung und ohne jedes weiteres Zuwarten, also noch bevor der Hausdurchsuchungsbefehl auch nur annähernd durchgelesen werden konnte, in das Großraumbüro, in welchem unter anderem auch der Einkaufsbereich situiert ist. Ein Teil der Bediensteten der BWB sowie deren Hilfskräfte begaben sich in die Abteilung des Filialvertriebes.

Unmittelbar nach Erreichen des Einkaufsbereichs - das heißt, noch bevor die Mitarbeiter von XXXX in der Lage waren, den Hausdurchsuchungsbefehl durchzulesen (!) -wurde mit Durchsuchungshandlungen begonnen. Auch ein Zuwarten mit dem Beginn von Durchsuchungshandlungen bis zum Eintreffen eines zwischenzeitig bereits verständigten Rechtsanwaltes wurde von der belangten Behörde entgegen dem ausdrücklichen Ersuchen von XXXX abgelehnt, obwohl dieses Eintreffen innerhalb weniger Minuten erwartet wurde und auch tatsächlich stattfand.

Die BWB hat sohin mit Durchsuchungshandlungen begonnen, bevor die gem § 12 Abs 5 WettbG zwingend vor einer angeordneten Hausdurchsuchung durchzuführende Befragung zu den Voraussetzungen stattgefunden hat. Auch hat die belangte Behörde es unterlassen, XXXX den Untersuchungsgegenstand und/oder die Unterlagen, nach denen gesucht wird zu nennen. Die belangte Behörde hat XXXX daher keine Gelegenheit gegeben, das Gesuchte freiwillig herauszugeben.

Wie bereits dargelegt, war der Untersuchungsgegenstand gemäß dem Hausdurchsuchungsbefehl ausschließlich auf die Brauereiwirtschaft und auf Produkte der Brauereiwirtschaft und sohin das Biersortiment beschränkt. Insbesondere zu Beginn der Hausdurchsuchung erfolgten Durchsuchungshandlungen ohne jegliche inhaltliche Einschränkung.

6. Einsatz einer Spionage-Software durch die BWB

6.1

Einige BWB-Bedienstete samt Hilfskräften - mindestens fünf bis sechs Personen - begaben sich sogleich mit Betreten des Großraumbüros in den dort befindlichen Arbeitsbereich des XXXX-Mitarbeiters XXXX. Zu diesem Zeitpunkt arbeitete XXXX angemeldet an seinem Laptop; es war keine Passwortsperre aktiviert. XXXX wurde weder zu Beginn der Durchsuchung noch in deren weiteren Verlauf aufgefordert, sein Passwort bekanntzugeben oder bestimmte Dokumente/Korrespondenz herauszugeben.

Als angemeldeter Benutzer hat man Zugriff auf diverse personenbezogene Daten des jeweiligen Mitarbeiters sowie auch auf im Unternehmensnetzwerk gespeicherte personenbezogene Daten der XXXX-XXXX. An persönlichen Daten sind u.a. Adress- und Telefonbücher sowie (persönliche) E-Mails (jedenfalls auch solche, die den Untersuchungsgegenstand nicht umfassen) betroffen. Über lokale elektronische Arbeitsplätze wie den Laptop von XXXX können jedoch auch auf finanzielle und wirtschaftliche Kennzahlen (etwa Umsatzdaten, Soll-Ist-Vergleiche, etc), Berichte und Prognosen, Kunden- und Lieferantenbeziehungen, Informationen aus den Bereichen Produktion und technische Ausstattung sowie betriebliche Abläufe und wirtschaftliche Beziehungen zugegriffen werden. Es versteht sich aufgrund des sowohl in persönlicher, als auch sachlicher Hinsicht eingeschränkten Untersuchungsgegenstandes von selbst, dass der weitaus überwiegende Teil dieser Unterlagen und Daten nicht vom Untersuchungsgegenstand, der auf den Sortimentsbereich Bier eingeschränkt war, umfasst war.

Mit Betreten seines Arbeitsbereiches durch die BWB wurde XXXX aufgefordert, seinen Arbeitsplatz zu verlassen. XXXX hat sich in Befolgung dieses Befehls unverzüglich von seinem Arbeitsplatz erhoben. Eine BWB-Bedienstete, XXXX, setzte sich sofort zu dem Laptop und fragte, wie bestimmte Unterlagen am PC

abgelegt sind und wo sich die Schreiben von einer weiteren XXXX-Einkaufsmitarbeiterin, XXXX aus der Hauptzentrale in XXXX, befinden. Zwei der anwesenden Personen der BWB haben parallel bereits mit der Durchsuchung von physischen Ordnern begonnen.

Die gesamte Situation war zu diesem Zeitpunkt aufgrund der Vielzahl an anwesenden BWB-Bediensteten und deren Hilfskräften sowie der mehrfachen parallelen Durchsuchungshandlungen der BWB äußerst unübersichtlich. Auch wurde der gesamte Schreibtisch von XXXX von der BWB mit Ordnern vollgeräumt. Es war XXXX, insbesondere XXXX, somit unmöglich, sämtliche im Arbeitsbereich von XXXX vorgenommenen Durchsuchungshandlungen überwachen zu können.

Parallel dazu wurden auch bereits in weiteren Arbeitsbereichen des Großraumbüros und den übrigen Büroräumlichkeiten der XXXX, insbesondere im Bereich der XXXX-Einkaufsmitarbeiterin XXXX, Durchsuchungshandlungen von der BWB gesetzt.

6.2

Gegen ca. 10:55 Uhr bemerkte XXXX, dass an seinem Laptop an einem USB-Port seines Laptops ein ihm unbekanntes Gerät angesteckt war. Dieses Gerät war im Zeitpunkt, als er von der BWB aufgefordert wurde, seinen Arbeitsplatz zu verlassen, noch nicht angesteckt. Über diese Maßnahme, also weder über die Tatsache, dass ein USB-Gerät an den Laptop angeschlossen wurde, noch um welches Gerät bzw um welche Software es sich hierbei handelt, noch was damit bezweckt bzw durchgeführt wurde, ist weder XXXX noch XXXX informiert worden. Wie lange das USBGerät angeschlossen war, kann aus Sicht von XXXX nicht mehr im Detail rekonstruiert werden. Insbesondere während der Hausdurchsuchung verfügte XXXX mangels Auskunft durch die BWB daher über keinerlei Informationen, um welches Gerät es sich handelte, wann und von wem das Gerät an den Laptop von XXXX angesteckt wurde, welche Programme und Funktionen ausgeführt wurden und welche Daten mit Hilfe dieses Gerätes verarbeitet - insbesondere welche Unterlagen kopiert - und übermittelt wurden.

Um MEST 11:02 Uhr hat die konzernale Antiviren-Software von XXXX eine Attacke gegen den Rechner von XXXX registriert, protokolliert und auf dieses Ereignis reagiert. Nach Information der XXXX Antiviren-Software handelte es sich um eine Schadsoftware, die mittels Passwort-Cracker versuchte, Zugang zu geschützten Daten zu erlangen.

Diese Meldung der XXXX-Antiviren-Software war dringender Anlass für weitere Nachforschungen, da zu diesem Zeitpunkt weder bekannt war von wem, noch wie lange das Gerät am Laptop von XXXX angesteckt war und welche Bedrohung davon für die IT-Infrastruktur der XXXX-XXXX, in der ca. 80 bis 100 Gesellschaften im In-und Ausland miteinander verbunden sind, ausgeht. Darüber hinaus wurde dieser Umstand in den Anmerkungen zu dem von der BWB geführten Protokoll über den Ablauf der Hausdurchsuchung gerügt. Es ist zu betonen, dass die BWB während der gesamten Hausdurchsuchung über diesen Vorfall XXXX nicht informiert hat und den Einsatz einer Software (die - wie im Folgenden dargestellt wird - als illegal einzuordnen ist), erst auf Nachfrage von XXXX zu einem späteren Zeitpunkt zugestanden hat (siehe sogleich).

6.3

Um das exakte Bedrohungspotential der eingesetzten Schadsoftware abklären zu können wurde noch am 20.08.2013 der allgemein beeidete und gerichtlich zertifizierte Sachverständige für die Fachgebiete IT-Sicherheit, Datenschutz, Verschlüsselung und Signaturerstellung, Virenschutz, forensische Datensicherung, Datenrekonstruktion und Datenauswertung XXXX von XXXX mit der Beweissicherung beauftragt und ihm zu diesem Zweck der Laptop von XXXX übergeben.

Um überprüfen zu können, um welche Schadsoftware es sich handelte und welche Schäden diese bereits verursachte bzw noch verursachen kann, wurden mit Schreiben der Vertreterin der Beschwerdeführer vom 21.08.2013 entsprechende Informationen von der BWB angefordert. Konkret wurden nachstehende Informationen und Unterlagen angefordert:

Welche Programme haben sich auf jenem USB-Gerät befunden, welches am 19.08.2013 beim Laptop von XXXX in XXXX von der BWB angeschlossen wurde?

Welche Programme wurden hievon innerhalb der konzernalen IT-Infrastruktur von XXXX ausgeführt und welche Geräte von XXXX waren davon betroffen?

Welche Informationen wurden von diesen Programmen aufgezeichnet und welche sensible Benutzerdaten (zB Passwörter, personenbezogene Daten - dies auch vor dem Hintergrund der Informationspflichten und Betroffenenrechten nach DSG etc) wurden erfasst, wobei wir insbesondere die Log-Files, etwaige Konfigurationsdateien und die Schadsoftware selbst benötigen?

Eine Dokumentation der Schadsoftware in Form eines (elektronischen) Benutzerhandbuches.

Von der BWB wurde diesbezüglich eine Auskunft von dem BKA als deren Hilfsorgan

eingeholt und an XXXX weitergeleitet. In dieser wurde mitgeteilt, dass lediglich die Programme "DumplT sowie "osTriage" ausgeführt worden wären. Das BKA behauptet jedoch, dass der installierte Virenscan die Ausführung des Programms verhindert hätte und deshalb vor Abschluss des Scans das Programm vom BKA beendet worden wäre. Wie sich nachträglich herausstellte, ist diese Behauptung des BKA unrichtig.

Weitere Informationen wurden seitens der BWB jedoch verweigert. Insbesondere wurde die geforderte Dokumentation nicht geliefert. Es wurde jedoch ein einseitiger Auszug aus dem Benutzerhandbuch zum Programm osTriage übermittelt. Aus diesem ergibt sich, dass das Programm vom FBI entwickelt wurde. Des Weiteren ergibt sich aus diesem Benutzerhandbuch, dass das Programm osTriage zumindest über nachstehende Funktionen verfügt:

Anzeige des Browser-Historie von Internet-Browsern

Dekodierung von Ank-Files und Anzeige verschiedener Daten und Uhrzeiten, Zielordner, Quelllaufwerke etc.

liest Passwörter aus

liest Chat-Nachrichten aus

extrahiert eine Liste der letzten geöffneten Daten(banken)

durchsucht mehrere Laufwerke

vergleicht automatisch gefundene Bilder und Videos mit einer rund 600.000 SHAs umfassenden Vergleichsdatenbank

überprüft Datei-Namen anhand einer Liste von mehr als 300 Schlüsselwörtern

kann Screen-Shots anfertigen

protokolliert sämtliche Aktivitäten

ermöglicht das Kopieren von Fotos und Videos

ermöglicht spezifizierte Suchvorgänge und der Kopie der hierbei gefundenen Dateien

durchsucht und öffnet zip-, rar- und 7z-Archive-Dateien

Es handelt sich daher bei dem von der BWB im Wege über ihre Hilfskräfte des BKA eingesetzte Software um eine vom FBI entwickelte und eingesetzte Spionagesoftware. Es ist daher davon auszugehen, dass sich die Vergleichsdatenbank in den USA befindet.

In weiterer Folge fand aufgrund dieses Aufforderungsschreibens am 21.08.2013 in der Zeit zwischen 19:30 und 20:35 Uhr eine Telefonkonferenz zwischen XXXX-Mitarbeitern, Rechtsvertretern von XXXX, Bediensteten der BWB, dem stellvertretenden Leiter der Forensikabteilung des BKA sowie dem Sachverständigen XXXX statt.

Bei dieser Telefonkonferenz wurde seitens der XXXX-IT darauf hingewiesen, dass laut Protokoll der XXXX-Antiviren-Software das Programm "MSpass.exe" ausgeführt wurde. Hiebei handelt es sich um ein bekanntes Programm für ein Instant-Messenger-Password-Recovery, welches ein Programmteil von osTriage ist. Laut SV

XXXX ist das Programm osTriage im "Schrotflintenmodus" ausgeführt worden, um möglichst breit zu suchen. osTriage stelle wiederum eine Programmsammlung dar.

Daraufhin wurde vom BKA ausdrücklich zugesagt, die forensischen Pfade der eingesetzten Tools bekanntzugeben und eine Übersicht/Zusammenfassung der Dateien, die extrahiert wurden, zur Verfügung zu stellen. Gleichzeitig wurde vom BKA zugestanden, dass das BKA keine gesicherte Information darüber hat, über welche Funktionen die eingesetzten Tools im Detail verfügen und welche Dateien daher aufgerufen, durchsucht und allenfalls kopiert wurden. Eine entsprechende Unterstützung, die erforderlichen Informationen vom Hersteller des Programmes zu erlangen wurde vom BKA jedoch abgelehnt. Über ausdrückliches Nachfragen, ob die BWB bzw das BKA garantieren können, dass das eingesetzte Tool keine Schäden im IT-System von XXXX anrichtet bzw. angerichtet hat, wurde dies seitens des BKA mit dem Hinweis verneint, dass das BKA einerseits eben keine Kenntnis darüber habe, welche Programme gestartet und welche Funktionen aufgerufen werden; andererseits habe das BKA keine Kenntnis über die exakten Spezifikationen der XXXX-IT. Besonders bemerkenswert ist die Mitteilung des BKA, dass das eingesetzte Programm bei einem Testlauf von der Firewall bzw der Anti-Viren-Software des BKA nicht erkannt wurde. Demzufolge ist das Programm spezifisch darauf ausgelegt, von Anti-Viren-Programmen und/oder Firewall nicht erkannt zu werden. Im Zuge dieser Telefonkonferenz wurde von der BWB auch ausdrücklich eingestanden, dass ihr die Bestimmungen des DSG nicht bekannt sind!

Die Übergabe des USB-Sticks im Original samt den darauf befindlichen Programmen und gespeicherten Daten sowie des entsprechenden Handbuches für das Programm osTriage oder einer Kopie hievon wurden seitens des BKA mit Hinweis auf fehlende Urheberrechte (in Bezug auf das Handbuch) abgelehnt. Auch die bloße Einsichtnahme in das Handbuch wurde nicht gewährt.

Über Nachfragen von XXXX, ob eine Autorisierung des Einsatzes des Tools erfolgte bzw auf welcher Rechtsgrundlage der Einsatz erfolgte, wurde seitens des BKA entgegnet, dass eine Autorisierung nicht notwendig wäre. Von der BWB wurde zugestanden, dass der Einsatz solcher Programme im Gesetz nicht ausdrücklich geregelt ist, jedoch behauptet, dass der Einsatz vom Hausdurchsuchungsbefehl umfasst gewesen wäre. Vom BKA wurde bestätigt, dass die Schlag- bzw Schlüsselwörter für das Tool von der BWB als Auftraggeber zur Verfügung gestellt wurden und das BKA als Hilfsorgan im Auftrag der BWB gehandelt hatte. Über ausdrückliches Nachfragen seitens XXXX, wer konkret den Auftrag zum Einsatz des Tools erteilt habe, wurde seitens der BWB auf die monokratische Organisationsstruktur der BWB verwiesen. Die BWB hat sohin den Einsatz eines Gerätes beauftragt, über deren genauen Inhalt und Funktion weder sie selbst noch ihr Hilfsorgan Bescheid wussten und über welches keine gesicherten Informationen vorhanden waren und sind.

6.4

Entgegen der von der belangten Behörde in der Telefonkonferenz vom 21.08.2013 gemachten Zusicherung wurden die zugesagten Informationen nicht übermittelt. Dies trotz mehrmaligen Urgierens und des Hinweises auf die für die IT der XXXX-XXXX bestehende Bedrohung. Von der belangten Behörde wurden lediglich die Seriennummer sowie die Bezeichnung des eingesetzten USB-Sticks bekanntgegeben. Wie sich jedoch nachträglich herausstellte, stimmte die von der BWB bekanntgegebene Seriennummer des USB-Sticks mit der Setup ap.dv Log-Datei nicht überein.

6.5

SV XXXX wurde - wie bereits ausgeführt - mit der Beweissicherung und der Einschätzung des sich aus dem Anschließen des USB-Sticks ergebenden Risikos hinsichtlich der Integrität und Stabilität der IT-Systeme von XXXX beauftragt.

Dem SV XXXX war es möglich, zu verifizieren, dass der gegenständliche USB-Stick am 19.08.2013 zumindest von 10:56 Uhr bis 11:35 Uhr am System der XXXX angeschlossen war. Dass der USB-Stick auch darüber hinaus angeschlossen war, kann jedoch nicht ausgeschlossen werden.

Des Weiteren konnte SV XXXX anhand einer forensischen Analyse feststellen, dass von dem gegenständlichen USB-Stick zumindest zwei Passwortentschlüsselungsprogramme aufgerufen wurden, wobei das aufrufende Programm osTriage.exe war. Bei den Passwortentschlüsselungsprogrammen handelt es sich um die Programme "mspass.exe" und "iepv.exe" des Herstellers Nirsoft. Letztgenanntes Programm extrahiert Passwörter, die im Kontext des Microsoft Internet Explorers abgespeichert sind.

Darüber hinaus spricht laut dem SV XXXX vieles dafür, dass weitere Programme aufgerufen wurden.

osTriage ist eine Sammlung von mitunter forensischen Programmen, die wiederum eine Reihe von Programmen anderer Hersteller aufruft. Bestandteil von osTriage sind zudem auch Programme, welche nicht für eine forensische Standard-Software üblich sind. Damit sind vor allem die Cracking-Tools des Herstellers Nirsoft gemeint, die der Überwindung von diversen Systembarrieren (Auslesen von Kennwörtern verschiedener Browser-Applikationen, Auslesen von Passwörtern verschiedener Kommunikationsdienste, Auslesen von Informationen über das persönliche Benutzerverhalten, Angriffe auf die Antiviren-Software etc) dienen. Das heimliche Auslesen von Daten, wie Kennwörtern des Benutzers, ist eines der Charakteristiken von Spionage-Software. Dementsprechend werden auch die Programme des Herstellers Nirsoft vom Hersteller von Antiviren-Software (Trendmicro) als Spionage-Software klassifiziert.

Zusammenfassend gelangte es dem SV XXXX am Schluss, dass osTriage und die weiteren nachgewiesenen Software-Tools sich jedenfalls zum Auskundschaften von Geheimnissen, welche in Form von digitalen Daten vorliegen, eignet.

osTriage ist derart konzipiert, dass es seine Operationen selbst dann nicht abbricht, wenn mspass.exe von der Virenschutzsoftware gelöscht oder geblockt wird. Zudem ist osTriage ein äußerst schnell arbeitendes Programm. Aus diesem Grunde sind bereits wenige Minuten ausreichend, um das Programm vollständig durchlaufen zu lassen. Da der USB-Stick jedoch mindestens eine halbe Stunde angesteckt war, ist diese Dauer bei weitem ausreichend, um eine Fülle von Daten zu sammeln, Unterlagen zu kopieren und das Programm vollständig durchlaufen zu lassen. Es ist daher die Stellungnahme der BWB bzw des BKA, wonach die Ausführung des Programms osTriage abgebrochen wurde, objektiv unrichtig.

Aufgrund dieses Umstandes ist konnte zunächst auch nicht ausgeschlossen, dass ein anderes Tool der BWB die WLAN-Schlüssel ausgelesen hat. Mit diesen Schlüsseln ist der jederzeitige Zugriff auf das Unternehmensnetzwerk von XXXX möglich. Daher wurden die entsprechenden WLAN-Schlüssel als kompromittiert angesehen und empfahl der Sachverständige, die betroffenen Schlüssel sofort zu ändern. Aufgrund weiterer Überprüfungen und Simulationen gelangte SV XXXX zur Überzeugung, dass mangels Administratorenrechten ausgeschlossen werden- konnte, dass die WLAN-Schlüssel mit Tools vor Ort entschlüsselt worden sind. Es kann aber nach wie vor nicht ausgeschlossen werden, dass die WLAN-Schlüssel in verschlüsselter Form kopiert wurden, wobei eine derartige Verschlüsselung nachträglich angegriffen werden kann.

osTriage ist primär für den Einsatz bei der Bekämpfung von Kinderpornographie entwickelt worden. Aus diesem Grunde beinhaltet es auch die Funktion, dass geöffnete Daten automatisch mit einer Vergleichsdatenbank abgeglichen werden.

Weiters konnte verifiziert werden, dass das Programm "DumplT eingesetzt wurde. DumpIT ist eine Software zum Zugriff auf die im Arbeitsspeicher enthaltenen Daten. Bei DumpIT handelt es sich nicht um eine forensische Standard-Software, sondern um ein, aus der Cracking-Szene herausentwickeltes, Incident Response Tool, dass Systembarrieren überwindet. Mit diesem Programm wird ein Zugriff auf Schlüssel und Passwörter, die im Arbeitsspeicher abgelegt sind, versucht. Dies stellt einen schwerwiegenden Eingriff in die Integrität eines Systems dar, da die vertraulichen Schlüssel kompromittiert sind, wenn dieser Zugriff gelingt. Unabhängig davon, ob der Einsatz dieser Software erfolgreich war oder nicht, war er jedenfalls nicht notwendig, da die Bediensteten der BWB und deren Hilfskräfte als am System angemeldete Benutzer des Laptops von XXXX Zugriff auf das bereits entschlüsselte Dateisystem hatten.

Darüber hinaus kam das Programm "Unlocker" zur Anwendung. Unlocker ist eine Software, die den Zugriff auf gesperrte Dateien erlaubt, indem sie die Sperre aufhebt. Die so entsperrten Dateien können dadurch kopiert werden. Dies kann beispielsweise auf die Auslagerungsdatei (pagefile.sys) und die Ruhezustandsdatei (hiberfil.sys) angewendet werden, um an Schlüsselmaterial zu gelangen, die in diesen Dateien abgelegt ist. Aufgrund des Umstandes, dass das BKA selbst über keine gesicherten Informationen über die Funktionen und aufgerufenen Dateien des Programms verfügt, kann nicht ausgeschlossen werden, dass die vorgenannten Dateien (hiberfil.sys und pagefile.sys) kopiert wurden. Auch der Einsatz dieser Software wäre nicht notwendig, da die Sicherung von Schlüsselmaterial nicht geboten war. Der Einsatz dieser Software hatte jedenfalls zur Folge, dass die Bitlocker-Verschlüsselung des Systems als kompromittiert anzusehen ist und das Notebook daher nicht mehr verwendet werden kann. Der Grund ist in der nicht mehr vorhandenen Integrität des Systems zu sehen und bietet die Festplattenverschlüsselung keinen Schutz mehr vor dem Verlust vertraulicher Daten.

Schließlich musste auch festgestellt werden, dass die von der BWB bekanntgegebene Seriennummer des USB-Sticks mit der laut setupapi.dev Logdatei nicht übereinstimmt.

13

Ohne eine genaue Aufstellung der Programme, die auf dem USB-Stick abgelegt waren, mit der zugehörigen md5-hashes (Prüfsummen), dem vollständigen Handbuch von osTriage und einem forensischen Image des USB-Sticks, sodass die Programme und die Reaktionen nachvollzogen werden können, ist eine genaue Abschätzung, welche Programme oder Dateien aufgerufen bzw ausgeführt wurden und sohin welche Daten und Unterlagen von XXXX und/oder deren Mitarbeiter verarbeitet wurden und an welche allfälligen Empfänger diese übermittelt wurden nicht möglich. Dies bedingt natürlich auch, dass eine Abschätzung des weiteren Risikos bislang nicht möglich ist.

Abschließend ist darauf zu verweisen, dass osTriage seine Vorgänge grundsätzlich in einer Protokolldatei aufzeichnet. Sollte eine Aufzeichnung jedoch nicht erfolgt sein, wovon nach dem derzeitigen Kenntnisstand auszugehen ist, so weist dies auf eine mangelnde Stabilität und Eignung dieser Software hin. Ein nicht dokumentierter Einsatz ist aus den aufgezeigten Gründen äußerst problematisch.

7.

Outlook-Postfächer von XXXX-Mitarbeitern

Parallel zu dem zu Punkt 11.6 dargestellten Einsatz der Spionagesoftware wurde von der belangten Behörde verlangt, dass die gesamten Shares (Netzwerksverzeichnisse) mit der Bezeichnung ZN06-700 und ZN06-710 und die gesamten Outlook-Postfächer der XXXX-Mitarbeiter XXXX, XXXX und XXXX auf eine von der BWB mitgebrachte externe Festplatte kopiert werden.

In der XXXX XXXX sind jedoch keine elektronischen Daten physisch gespeichert, die vom Untersuchungsgegenstand umfasst sind. Diese befinden sich auf den Servern im XXXX-Rechenzentrum in der Hauptzentrale in XXXX.

Trotz ausdrücklichen Hinweises auf diesen Umstand hat die belangte Behörde die Kopien der gesamten Shares mit der Bezeichnung ZN06-700 und ZN06-710 auf eine von der belangten Behörde mitgebrachte externe Festplatte verlangt. Diese Netzwerkverzeichnisse beinhalten jedoch uneingeschränkt sämtliche Office-Dokumente wie zB Word, EXCEL, Power Point, etc der beiden genannten Einkaufsabteilungen (ZN06- 700 und ZN06-710). Der Datenbestand dieser beiden Shares ist daher zum überwiegenden Teil vom Untersuchungsgegenstand und vom örtlichen Anwendungsbereich des Hausdurchsuchungsbefehls des KG vom 06.08.2013 zur Gänze nicht umfasst. Insbesondere können die beiden vorgenannten Netzwerkverzeichnisse auch Daten von Mitarbeitern enthalten, die das Unternehmen zwischenzeitig bereits verlassen haben.

XXXX hat daher unter Berufung auf die Versiegelungsgründe der Überschreitung des Untersuchungsgegenstandes sowie der gesetzlich anerkannten Verschwiegenheitspflicht nach dem DSG die Versiegelung des Datenbestandes ausgesprochen und gem § 12 Abs 6 WettbG die Bildung von Gruppen von Unterlagen beantragt. Ausdrücklich wurde die Überschreitung des Untersuchungsgegenstandes und die Verletzung der DSG gerügt.

Die BWB hat jedoch die Versieglung nicht anerkannt und unter ausdrücklicher Androhung der Anwendung behördlicher Zwangsgewalt die Übergabe des Datenbestandes befohlen und durchgeführt. Es wurde sohin eine Kopie der Shares mit der Bezeichnung ZN06-700 und ZN06-710 auf einen von der belangten Behörde mitgebrachten externen Festplatte gespeichert. Diese externe Festplatte wurde von der belangten Behörde am 19.08.2013 unversiegelt und ungesichert in Gewahrsam genommen.

Erst am 20.08.2013 um 16:32 Uhr wurde XXXX mitgeteilt, dass die auf der externen Festplatte befindlichen Daten gelöscht werden sollen. Über ausdrückliches Nachfragen von XXXX wurde die Löschung über Anweisungen und im Beisein der belangten Behörde von XXXX um 16:33 Uhr jedoch nicht durch Formatierung, sondern lediglich durch ein normales Löschkommando vorgenommen. Die externe Festplatte ist von der belangten Behörde in diesem Zustand wieder mitgenommen worden.

Mail-for-Exchange-Daten von XXXX-Mitarbeitern

Zusätzlich zu den Shares mit der Bezeichnung ZN06-700 und ZN06-710 hat die belangte Behörde - wie bereits dargelegt wurde - auch die uneingeschränkte Herausgabe der Mail-for-Exchange-Daten der XXXX-Mitarbeiter XXXX, XXXX und XXXX (dieser ist jedoch bereits bei 31.12.2012 pensionsbedingt aus dem Unternehmen ausgeschieden; die BWB wurde über diesen Umstand auch ausdrücklich aufgeklärt) im Format ".pst" durch Export am lokalen Outlook-Client gefordert. Es sind jedoch auch diese elektronischen Daten nicht in der XXXX

XXXX physisch gespeichert, sondern befinden sich ebenfalls auf den Servern im Rechenzentrum in der Hauptzentrale in XXXX. Darüber hinaus wird die Erstellung einer solchen Datei im Format ".pst" am lokalen Outlook-Client aus Sicherheitsgründen durch eine Standard-Security-Policy verhindert. Es hat daher auch die lokale IT der XXXX XXXX diesbezüglich sicherheitsbedingt keine systemische Berechtigung und daher mangels Berechtigung keine technische Möglichkeit die entsprechende Datei zu erstellen. Dies aus dem Grund, da es keinen Anwendungsfall gibt, der eine solche Funktionalität in einer Zweigniederlassung rechtfertigen würde.

Die BWB wurde auch auf diesen Umstand ausdrücklich hingewiesen. Es wurde daher seitens XXXX auch hinsichtlich dieser Daten die Versieglung unter Berufung auf die Versiegelungsgründe der Überschreitung des Untersuchungsgegenstandes sowie der gesetzlich anerkannten Verschwiegenheitspflicht nach dem DSG ausgesprochen und erneut gem § 12 Abs 6 WettbG die Bildung von Gruppen von Unterlagen beantragt.

Über Nachfrage der BWB wurde diese darüber informiert, dass es in der XXXX XXXX lokal möglich wäre, eine Datei im Format ".ost" zu erstellen. ".ost"-Dateien können wie auch ".pst"-Dateien inhaltlich nicht eingeschränkt werden. Jeglicher Export der Exchange-Daten vom lokalen Outlook-Client in eine Datei - daher sowohl ein Export im „.pst"-als auch im ".ost"-Dateiformat - setzt sohin technisch zuvor ein Abrufen der Exchange-Daten vom zentralen Server in XXXX voraus.

Aus diesen und den vorgenannten Gründen wurde daher auch hinsichtlich der ".ost"- Datei die Versiegelung ausgesprochen. Um weitere Verzögerungen zu vermeiden wurde die ".ost"-Datei jedoch seitens XXXX bereits erstellt. Die Übernahme besagter ".ost"- Datei wurde von der BWB jedoch mit dem Argument abgelehnt, dass sie eine Datei im ".ost"-Format nicht verarbeiten könne. Es handelt sich aber bei ".ost"-Dateien um ein allgemein gebräuchliches Dateiformat.

Vernehmung von XXXX-Mitarbeitern als Zeugen

Am 19.08.2013 ab ca 17:00 Uhr führte die BWB zeugenschaftliche Einvernahmen der XXXX-Mitarbeiter XXXX, XXXX und XXXX durch. Im Rahmen dieser Einvernahmen wurde XXXX ein Anmerkungs- und Zeugenbefragungsrecht von der belangten Behörde ausdrücklich verweigert.

Zu Beginn der jeweiligen Zeugeneinvernahmen hat die belangte Behörde die Zeugen auch nicht darauf hingewiesen, dass sie nicht verpflichtet sind, die verlangten Auskünfte zu erteilen und daher berechtigt sind, die Aussage zu verweigern.

Bei der Einvernahme der XXXX-Mitarbeiter XXXX und XXXX wurde den Zeugen jeweils die Beilagen ./C und ./D zum Antrag der BWB auf Erlassung eines Hausdurchsuchungsbefehls vorgehalten und jeweils die Frage gestellt, wie sie es sich erklären können, dass diese bei der Hausdurchsuchung nicht gefunden werden können. Dieser Vorhalt war jedoch grob unrichtig, da die vorgenannte Vorlage ./D als Seite 514 Bestandteil der von der BWB kopierten bzw ausgedruckten Dokumenten ist.

Auch wurden die Niederschriften über die Einvernahme der vorgenannten Zeugen weder verlesen noch zur Durchsicht vorgelegt, obwohl ein Verzicht hierauf nicht erklärt wurde. Erst im Rahmen der Beendigung der Hausdurchsuchung wurden XXXX Protokolle übergeben, aus denen ersichtlich war, dass die Zeugeneinvernahmen nicht im Rahmen der Hausdurchsuchung protokolliert wurden.

Die Hausdurchsuchung wurde am 19.08.2013 gegen 21:00 Uhr unterbrochen und die Fortsetzung für den nächsten Tag angekündigt.

10.

Weitere Vorkommnisse

Am 19.08.2013 wurden von BWB-Bediensteten und deren Hilfskräften mit fototauglichen Handys (Smartphones) Fotos angefertigt. Da die BWB bereits im Rahmen der im Jänner und Februar 2013 in der XXXX-Hauptzentrale stattgefundenen Hausdurchsuchung mitgeteilt hat, dass die BWB-Bediensteten über keine Diensthandys verfügen, hat XXXX Auskunft darüber verlangt, ob es sich bei diesen Handys nunmehr nach wie vor um Privat- oder um Diensthandys handelt. Eine diesbezügliche Auskunft wurde verweigert. XXXX hat daraufhin verlangt, die Frage und die Verweigerung der Auskunft zu protokollieren. Es wurde jedoch auch dieses Begehren von der BWB begründungslos verweigert.

Schließlich hat die BWB auch unrichtig protokolliert, dass die bereits näher dargestellten Postfächer und Shares sich nicht auf den zuletzt bei der in der Hauptzentrale durchgeführten Hausdurchsuchung sichergestellten Sicherungsbändern befänden. Diese Aussage wurde seitens XXXX in dieser Form jedoch nicht getätigt. Tatsächlich hat XXXX mitgeteilt, dass die Sicherungskopien der Mail-for-Exchange-Daten (Outlook) per 31.12.2012 auf dem Jahressicherungsband für das Jahr 2012 befinden, welches bei der Hausdurchsuchung der Hauptzentrale in XXXX bereits kopiert wurde. Hinsichtlich der Mail-for-Exchange-Daten seit 01.01.2013 sowie hinsichtlich der beiden angeforderten Shares mit der Bezeichnung ZN06-700 und ZN06-710 hat XXXX mitgeteilt, dass sich diese noch nicht in elektronischer Form bei der BWB bzw dem Kartellgericht befinden. Eine Richtigstellung der entsprechenden Protokollierung wurde von der belangten Behörde ebenfalls verweigert.

Untätigkeit der BWB am 20.08.2013 in XXXX

Am 20.08.2013 wurde die Hausdurchsuchung in der XXXX XXXX nur mehr von lediglich zwei BWB-Bediensteten fortgesetzt; eine weitere, nicht operativ tätige BWB-Mitarbeiterin, XXXX, war zu Zwecken der Anfertigung von Kopien oder sonstiger Hilfstätigkeiten anwesend. Diese haben um 09:34 Uhr die XXXX betreten. Der Erstkontakt mit XXXX fand um 09:50 Uhr zur Entsiegelung des am Vorabend versiegelten Büros des XXXX-Mitarbeiters XXXX statt, in welchem Unterlagen von der BWB zwischengelagert wurden.

In weiterer Folge wurden von den anwesenden BWB-Bediensteten jedoch keinerlei weitere Untersuchungshandlungen gesetzt. Trotz mehrmaligen ausdrücklichen Nachfragens seitens XXXX wurden auch erst um ca 14:45 Uhr die am Vortag von der BWB als potentiell relevant eingestufte Papierdokumente XXXX zur Durchsicht übergeben. Eine Begründung für diese Verzögerung wurde seitens der belangten Behörde nicht genannt.

Wie sich nachträglich herausstellte, wurde die Hausdurchsuchung in den Geschäftsräumlichkeiten der XXXX XXXX in XXXX XXXX, von der BWB aufgrund der rechtsirrigen Annahme, dass auch im Falle der "Fortsetzung" der Hausdurchsuchung in der Hauptzentrale in XXXX eine einheitliche Hausdurchsuchung vorliege, lediglich formal aufrecht erhalten. Dies ergibt sich aus dem Umstand, dass um ca 14:45 Uhr vier BWB-Bedienstete in der Hauptzentrale in XXXX eintrafen, sich inhaltlich auf den Beschluss des OLG Wien vom 06.08.2013 beriefen und ausdrücklich erklärten, die in der XXXX XXXX begonnene Hausdurchsuchung nunmehr in XXXX "fortzusetzen".

Um 16:51 Uhr haben die in der XXXX XXXX anwesenden BWB-Bediensteten eine Kopie des Protokolls der Hausdurchsuchung am Standort XXXX sowie die Niederschriften über die Einvernahmen der Zeugen XXXX, XXXX und XXXX an XXXX übergeben. Über ausdrückliches Nachfragen wurde seitens der belangten Behörde mitgeteilt, dass Anmerkungen zu diesen vorgenannten Niederschriften nicht möglich sind bzw von der BWB nicht protokolliert werden.

Es ist auch anzumerken, dass von der BWB die beiden Niederschriften über den Gang der Hausdurchsuchungen in XXXX und in XXXX nachträglich zu einem Protokoll zusammengeführt wurden.

Hausdurchsuchungsbefehl vom 20.08.2013

Am 20.08.2013 hat die BWB beim OLG Wien als KG einen Antrag auf "Erweiterung des Hausdurchsuchungsbefehls" gestellt und zwar möge das OLG Wien als KG den Hausdurchsuchungsbefehl zu 26 Kt 88/13 vom 06.08.2013 gemäß § 12 Abs 1 und 3 WettbG auf die Geschäftsräumlichkeiten der XXXX XXXXXXXXXXXX, alle in XXXX, zwecks Sicherstellung von physischen und elektronischen Kopien, ausdehnen. Mit Beschluss des OLG Wien vom 20.08.2013, 26 Kt 88/13-4, 26 Kt 101/13, 102/13, wurde der am 06.08.2013 zu 26 Kt 88/13-2 erlassene Hausdurchsuchungsbefehl antragsgemäß "erweitert."

13.

Beginn der Hausdurchsuchung am 20.08.2013 in XXXX

Als die BWB-Bediensteten am 20.08.2013 gegen 14:45 Uhr in der HZ eintrafen, wurde die Leiterin des konzernalen Rechtes Österreich, XXXX, von den am Empfang tätigen Mitarbeiterinnen von XXXX informiert. Anschließend wurden die BWB-Bediensteten von XXXX, DI XXXX und XXXX am Empfang begrüßt und in einen Konferenzraum im 5. Stock geführt.

Im Konferenzraum angekommen, teilte die BWB mit, dass sie über einen Beschluss des OLG Wien als KG verfüge, mit welchem der Hausdurchsuchungsbefehl vom 06.08.2013 personell auf die zweit- und

drittbeschwerdeführenden Parteien sowie räumlich auf die Geschäftsräumlichkeiten in XXXX, "erweitert" werde. Die Bediensteten der belangten Behörde hatten diesen Beschluss jedoch nicht physisch bei sich und erklärten, dass dieser "demnächst" zugestellt werden würde.

Anschließend erkundigte sich die BWB, ob es sich um die Geschäftsräumlichkeiten der beschwerdeführenden Parteien handelt und ob für diese Zustellbevollmächtigte anwesend sind. Weitergehende Fragen, insbesondere inhaltlicher Natur, wurden nicht gestellt. Hinsichtlich des Grundes der Hausdurchsuchung erklärte die BWB, dass die "Erweiterung" beantragt wurde, weil im Zuge der Hausdurchsuchung in XXXX die Versiegelung von elektronischen Daten mit der Begründung, dass diese physisch in der HZ gespeichert sind und daher vom örtlichen Anwendungsbereich des Hausdurchsuchungsbefehls vom 06.08.2013 nicht umfasst sind, ausgesprochen worden sei. Die belangte Behörde hat jedoch nicht mitgeteilt, nach welchen Dokumenten in der HZ gesucht wurde. Auch hat die BWB XXXX weder aufgefordert, noch Gelegenheit gegeben, das Gesuchte freiwillig herauszugeben.

Die belangte Behörde hat daher auch bei der Hausdurchsuchung in XXXX mit der Hausdurchsuchung, d.h. mit Durchsuchungshandlungen begonnen, bevor die gem § 12 Abs 5 WettbG zwingend vor einer angeordneten Hausdurchsuchung durchzuführende Befragung zu den Voraussetzungen stattgefunden hat. Auch hat die belangte Behörde es erneut unterlassen, XXXX den Untersuchungsgegenstand und/oder die Unterlagen, nach denen gesucht wird, zu nennen. Die belangte Behörde hat XXXX daher abermals keine Gelegenheit gegeben, das Gesuchte freiwillig herauszugeben.

14.

Anfertigung lediglich einer Kopie eines bekannten Dokuments

Seitens XXXX wurde darauf hingewiesen, dass die inhaltlichen Versiegelungsgründe aufrecht bleiben und wurde daher die Versiegelung, wie sie bereits zu Punkt 11.6 und Punkt 11.7 dargestellt wurde, angekündigt, wenn die BWB auf eine Kopie der elektronischen Daten besteht.

Daraufhin hat die belangte Behörde verlangt, dass ihr in die Outlook-Postfächer der XXXX-Mitarbeiter der XXXX XXXX XXXX und XXXX Einsicht gewährt wird. Die belangte Behörde begründete dies damit, dass sie überprüfen wolle, ob sie die Dokumente, die sie in den jeweiligen Postfächern in der XXXX XXXX vorgefunden hat, auch in der HZ vorfindet.

Nachdem diese einleitenden Bemerkungen seitens der BWB gemacht wurden, verließen die BWB-Mitarbeiter Dr. XXXX LL.M. und Ing. Mag. XXXX die Hauptzentrale von XXXX, weil sich Dr. XXXX LL.M. in ärztliche Behandlung geben musste; hiebei wurde er von Ing. Mag. XXXX begleitet.

In der Hauptzentrale von XXXX verblieben daher die BWB-Mitarbeiter Mag. XXXX und Mag. XXXX.

Sodann hat XXXX einen Zugang zu den beiden Postfächern hergestellt. Die Herstellung dieses Zuganges benötigte rund 45 Minuten, wobei von IT-Mitarbeitern von XXXX im erwähnten Konferenzraum zwei Laptops installiert wurden, auf welchen die von der BWB gewünschten Datenanwendungen (insbesondere Outlook) der XXXX-Mitarbeiter XXXX XXXX XXXX und XXXX direkt vom Server geladen wurden.

In diesem Zeitraum ist ein Bediensteter der belangten Behörde in das direkt neben der HZ situierte Einkaufszentrum XXXX gegangen. Nach dessen Rückkehr - ca 20 Minuten später - wurde XXXX der Beschluss des OLG Wien vom 20.08.2013 übergeben.

Nachdem die Installation der Datenanwendungen durch die XXXX-IT fertiggestellt worden war, haben sich die beiden verbliebenen BWB-Mitarbeiter vor die beiden Laptops gesetzt und im Outlook gestöbert. Sie haben erklärt, dass sie schauen wollten, ob sich hier der gleiche Outlook-Inhalt befindet wie in der Zweigniederlassung XXXX. Hiezu ist anzumerken, dass die beiden BWB-Mitarbeiter keine Listen über den Outlook-Inhalt in XXXX hatten, sodass es im Hinblick auf die Vielzahl der dort gelegten E-Mails äußerst unwahrscheinlich ist, dass hier ein Abgleich aus der Erinnerung möglich war.

Die belangte Behörde hat nach bereits 20 Minuten die Durchsuchungshandlungen der vorgenannten Outlook-Postfächer abgeschlossen. Die BWB hat hierbei ausschließlich nach der Beilage ./D zum Antrag auf Erlassung des Hausdurchsuchungsbefehles vom 02.08.2013 gesucht und ausschließlich dieses Dokument ausgedruckt. Die Beilage ./D wurde von der belangten Behörde jedoch bereits im Rahmen der Hausdurchsuchung in der XXXX XXXX gefunden und als Seite 514 unversiegelt zum Akt genommen.

Die BWB hat sich sohin des Mittels der Hausdurchsuchung bedient, um ausschließlich nach einem einzigen Dokument zu suchen, das bereits bei XXXX gefunden und unversiegelt zum Akt genommen wurde.

Darüber hinaus ist klarzustellen, dass ein Outlook-Posteingang unabhängig vom Ort des Zugriffes über den gleichen Inhalt verfügt. Es ist daher unerheblich, ob der Zugriff in der XXXX XXXX oder in der HZ erfolgt.

15.

Rekurse gegen die Hausdurchsuchungsbefehle

XXXX hat sowohl gegen den Beschluss des OLG Wien als KG vom 06.08.2013, 26 Kt 88/13-2, als auch gegen den Beschluss vom 20.08.2013, 26 Kt 88/13-4, 26 Kt 101, 102/13, Rekurs an den OGH als KOG erhoben.

Im Rekurs gegen den Beschluss vom 06.08.2013 wurde Nichtigkeit in Folge Verletzung des Rechtes auf den gesetzlichen Richter geltend gemacht. Im Rekurs gegen den Beschluss vom 20.08.2013 ist insbesondere geltend gemacht worden, dass eine "Erweiterung" eines bereits ergangenen Beschlusses rechtlich nicht möglich ist. Mit weiteren Rechtsmittelgründen wurde auch der Beschluss vom 20.08.2013 insbesondere wegen Vorliegen von Nichtigkeitsgründen angefochten.

16.

Notarielle Hinterlegung des Laptops

Nach forensischer Auswertung des Laptops von XXXX durch den SV XXXX hat dieser den gegenständlichen Laptop der Marke Lenovo T430, Inventarnummer P22636, Type 2349-2L3, Seriennummer PB-ZLRYG, zu Zwecken der Beweissicherung dem öffentlichen Notar Dr. XXXX mit dem Amtssitz in XXXX am 12.09.2013 übergeben. XXXX hat dem Notar den Auftrag erteilt, den Laptop zu versiegeln und den versiegelten Laptop zunächst in dessen Amtskanzlei zu verwahren und ausschließlich an XXXX oder an einen von XXXX schriftlich namhaft gemachten Dritten auszufolgen.

Die versiegelte Hinterlegung des Laptops erfolgte deshalb, damit in einem allfälligen Behördenverfahren einem anderen gerichtlich beeideten Sachverständigen der Laptop von XXXX in unveränderter Form vorgelegt werden kann.

[...]

IV.

RECHTSWIDRIGKEIT DER DURCHFÜHRUNG DER HAUSDURCHSUCHUNG

1.

Rechtslage

[...]

Hausdurchsuchungen sind Verwaltungsakte iSd § 67a Z 2 AVG

Der VfGH hat bereits klargestellt, dass wettbewerbsrechtliche Hausdurchsuchungen stets Zwangsmaßnahmen iSd § 67a Z 2 AVG darstellen, da die Hausdurchsuchung erforderlichenfalls mit Gewalt durchzusetzen wäre und ihr damit jedenfalls Zwangscharakter zukommt (VfGH 01.12.2012, B 619/12). Daran ändert - anders als von der belangten Behörde in einem anderen Verfahren fälschlich (und entgegen der zitierten Judikatur des VfGH) vermeint - nichts, dass einzelne Aktionen im Rahmen einer Hausdurchsuchung für sich nicht Zwangsakte darstellen. Es genügt der Kontext der Hausdurchsuchung und das von diesem ausgehende hoheitliche "Zwangspotential", damit eine Maßnahme zu einer Zwangsmaßnahme wird. Dies hat auch vorliegend zu gelten.

Gemäß Art 9 StGG iVm § 1 des Gesetzes zum Schutze des Hausrechtes, RGBI 1862/88 idgF, iVm § 12 Abs 1 und Abs 3 WettbG bedarf jede kartellrechtliche Hausdurchsuchung eines richterlichen Befehls. Die

Rechtsmäßigkeit einer Hausdurchsuchung setzt sohin zwingend voraus, dass diese aufgrund eines gültigen richterlichen Hausdurchsuchungsbefehls durchgeführt wurde (VfGH 01.12.2012, B619/12). Mit Maßnahmenbeschwerde anfechtbar sind daher (i) alle Hausdurchsuchungen, die ohne richterlichen Befehl durchgeführt wurden, (ii) all jene Handlungen, die keine Deckung im Hausdurchsuchungsbefehl finden oder (iii) zwar allenfalls im Hausdurchsuchungsbefehl Deckung finden, aber sonst nicht verhältnismäßig sind.

Rekurse gegen Hausdurchsuchungsbefehle

Wie oben dargelegt, hat XXXX gegen beide Hausdurchsuchungsbefehle, sohin sowohl gegen den Beschluss vom 06.08.2013, mit welchem die Durchführung einer Hausdurchsuchung in den Geschäftsräumlichkeiten in XXXX XXXX, angeordnet wurde, als auch gegen den Beschluss vom 20.08.2013, mit welchem der Beschluss vom 06.08.20113 personell auf die bisher im Verfahren nicht beteiligten Zweit-und Drittbeschwerdeführerinnen und räumlich auf die Geschäftsräumlichkeiten in XXXX, "erweitert" wurde, Rekurs an den OGH als KOG erhoben.

Da mit dem Beschluss vom 06.08.2013 über den verfahrenseinleitenden Antrag der BWB abschließend und vollständig entschieden wurde, ist das durch diesen Antrag eingeleitete Verfahren in I. Instanz abgeschlossen. Da einmal ausgefertigte Entscheidungen - mit Ausnahme hier nicht relevanten Berichtigungen und Ergänzungen - inhaltlich nicht mehr verändert werden können, ist das Gericht gern § 40 AußStrG an seine Beschlüsse gebunden. Eine Aufhebung oder auch nur Abänderung einer einmal ergangenen Entscheidung kommt daher nicht mehr in Betracht. Aus diesen Gründen ist die "Erweiterung" eines Beschlusses rechtlich nicht möglich.

Wird den von XXXX erhobenen Rekursen Folge gegebenen, so fällt in jedem Falle der richterliche Befehl, der Grundvoraussetzung für die rechtmäßige Durchführung einer Hausdurchsuchung ist, weg. Dass der Hausdurchsuchungsbefehl erst nachträglich beseitigt wird, spielt insoweit keine Rolle, als das Gesetz ausdrücklich eine aufschiebende Wirkung des Rekurses an den OGH als KOG ausschließt und daher insoweit die richterliche Kontrolle erst ex post wahrgenommen werden kann. Bei Wegfall der richterlichen Hausdurchsuchungsbefehle mangelt es sohin an der Grundvoraussetzung für die Rechtmäßigkeit der Durchführung einer Hausdurchsuchung.

Sind daher die von XXXX erhobenen Rekurse erfolgreich, fehlt den durchgeführten Hausdurchsuchungen die gesetzliche Grundlage und erfolgten diese sohin rechtswidrig. In einem solchen Falle stellt jedwede Maßnahme einen Maßnahmenexzess dar.

Vor diesem Hintergrund wird angeregt, das Verfahren bis zum Vorliegen der Entscheidungen OGH als KOG über die von XXXX erhobenen Rekurse gegen die Beschlüsse des OLG Wien vom 06.08.2013 und 20.08.2013 zu unterbrechen.

Die durchgeführten Hausdurchsuchungen sind zudem auch aus nachstehenden Gründen rechtswidrig:

4.

Verspätete Zustellung des Hausdurchsuchungsbefehls vom 06.08.2013

Hausdurchsuchungen stellen einen schwerwiegenden Eingriff in das verfassungsgesetzlich gewährleistete Hausrecht dar. Hausdurchsuchungen müssen daher sowohl in ihren Voraussetzungen als auch in ihrer Durchführung verhältnismäßig sein (Tipold/Zerbes, WK-StPO, Vor §§ 119 bis 122, Rn 9; VfGH 1.12.2012, B 619/12). So scheidet eine Hausdurchsuchung insbesondere bereits dann aus, wenn zur Klärung des Verdachtes gelindere Mittel zur Verfügung stehen (Wiederin in Korinek/Holoubek, BVG, Art 9 StGG, Rn 49). Des Weiteren erfordert die Verhältnismäßigkeit, dass die gesuchten Gegenstände bereits vor dem Eingriff bestimmt sein müssen, da eine Hausdurchsuchung zur bloßen Gewinnung von Verdachtsgründen grundsätzlich unzulässig ist (Tipold/Zerbes, aaO, Rn 10).

In diesem Zusammenhang ist es insbesondere erforderlich, dass der Hausdurchsuchungsbefehl - wie auch § 12 Abs 3 letzter Satz WettbG ausdrücklich normiert - den betroffenen Unternehmen sogleich oder doch innerhalb von 24 Stunden zuzustellen ist. Diesbezüglich hat die Behörde keine Wahlmöglichkeiten und muss die Zustellung des Hausdurchsuchungsbefehls daher innerhalb von 24 Stunden nach dem der Hausdurchsuchungsbefehl verkündet wurde erfolgen. Bereits das Unterlassen der fristgerechten Zustellung bedeutet daher eine Verletzung im verfassungsgesetzlich gewährleisteten Hausrecht (Wiederin, aaO, Rn 55; Tipold/Zerbes, WK-StPO altes Vomerfahren, § 140, Rn 7).

Das Erfordernis der Zustellung des Hausdurchsuchungsbefehls innerhalb von 24 Stunden ergibt sich bereits zweifelsfrei aus der mangelnden Befristung eines nach dem WettbG erlassenen Hausdurchsuchungsbefehls. Anders als § 105 StPO sieht § 12 WettbG kein Gebot einer Befristung eines Hausdurchsuchungsbefehls vor.

Wie jedoch zu Punkt 11.3 bis 11.5 dargelegt wurde, erfolgte die Zustellung des gegenständlichen Hausdurchsuchungsbefehles vom 06.08.2013 nicht innerhalb von 24 Stunden. Der Hausdurchsuchungsbefehl ist vom OLG Wien als KG am 06.08.2013 erlassen worden und von der belangten Behörde am 08.08.2013 übernommen worden. Die Zustellung hätte sohin spätestens am 09.08.2013 erfolgen müssen. Tatsächlich wurde der Hausdurchsuchungsbefehl den beschwerdeführenden Parteien erst am 19.08.2013 zugestellt. Bereits aus diesem Grunde liegt eine Verletzung im verfassungsgesetzlich gewährleisteten Hausrecht vor.

Der "Erweiterungs-Hausdurchsuchungsbefehl" vom 20.08.2013 wurde hingegen fristgerecht zugestellt.

Keine Prüfungsmöglichkeit durch XXXX Die belangte Behörde wäre jedoch auch verpflichtet gewesen, bei deren Eintreffen dem Unternehmen eine angemessene - wenn auch kurze - Frist einzuräumen, damit es mit Hilfe seiner Anwälte den Hausdurchsuchungsbefehl prüfen kann (EuG 06.09.2013, verbundene Rechtssagen T-289/11, T-290/11 und T-521/11, Deutsche Bahn AG, Rn 89).

Die Möglichkeit den Hausdurchsuchungsbefehl durchzulesen und mit Rechtsvertretern zu prüfen, ist unabdingbare Voraussetzung, damit das Unternehmen die Rechtsmäßigkeit und den Umfang der Hausdurchsuchung beurteilen kann. Die Beschwerdeführer räumen ein, dass die Prüffrist nicht lang sein muss. Vorliegend stand den Beschwerdeführern aber überhaupt keine Zeit zur Verfügung, sondern wurden die Durchsuchungshandlungen unmittelbar begonnen. Da die belangte Behörde jedoch auch dieser Verpflichtung nicht nachgekommen ist, sondern vielmehr mit der Hausdurchsuchung, dh mit Durchsuchungshandlungen, begonnen hat, bevor der Hausdurchsuchungsbefehl auch nur ansatzweise durchgelesen, geschweige denn anwaltlich geprüft werden konnte, hat die belangte Behörde auch aus diesem Grunde insbesondere das verfassungsgesetzlich geschützte Hausrecht der beschwerdeführenden Parteien verletzt.

Verstoß gegen § 12 Abs 5 WettbG Wie oben dargelegt, setzt die Verhältnismäßigkeit einer Hausdurchsuchung auch voraus, dass keine weniger belastende Maßnahme zur Verfügung steht. Vor diesem Hintergrund sind daher die betroffenen Unternehmen gern § 12 Abs 5 WettbG unmittelbar vor einer Hausdurchsuchung zu den Voraussetzungen der Hausdurchsuchung zu befragen. Im Zuge dieser Befragung sind die Betroffenen aufzufordern und ist den Betroffenen auch Gelegenheit zu geben, dass Gesuchte freiwillig herauszugeben (Tipold/Zerbes, WK-StPO, § 121, Rn 1 und Rn 2). Dies bedingt jedoch wiederum, dass die gesuchten Gegenstände bereits vor der Hausdurchsuchung ausreichend bestimmt sein müssen (Tipold/Zerbes, WK-StPO, Vor §§ 119 bis 122, Rn 10), da eine ausforschende Nachprüfung, eine sogenannte "Fishing Expedition", jedenfalls unzulässig ist. So stellt jede Inspektion von Dokumenten ohne besondere Begrenzung einen unverhältnismäßigen Eingriff in das verfassungsgesetzlich geschützte Hausrecht dar (Frowein in Frowein/Peukert, EMRK3, Art 8, Rn 45).

Da es die belangte Behörde jedoch unterlassen hat, vor der verfahrensgegenständlichen Hausdurchsuchung XXXX hinsichtlich der Voraussetzungen der Hausdurchsuchung zu befragen und sie aufzufordern und XXXX Gelegenheit zu geben, die gesuchten Gegenstände freiwillig herauszugeben, liegt auch aus diesem Grunde ein rechtswidriger Eingriff vor. Insbesondere ist an dieser Stelle bereits darauf hinzuweisen, dass die gesuchten Gegenstände vor dem Eingriff nicht ausreichend bestimmt waren. Tatsächlich handelte es sich bei der gegenständlichen Hausdurchsuchung um eine jedenfalls unzulässige Fishing Expedition. Dies ergibt sich bereits zweifelsfrei aus dem Umstand, dass die Hausdurchsuchung ohne eine besondere (inhaltliche) Begrenzung erfolgte; die verfahrensgegenständliche Hausdurchsuchung erstreckte sich vielmehr auf den gesamten Einkaufsbereich ohne jegliche Ausnahme. Die Hausdurchsuchung ist daher auch aus diesem Grunde jedenfalls als ein unverhältnismäßiger Exzess zu qualifizieren.

7.

Zeitlicher Exzess der Hausdurchsuchung in XXXX

Schließlich sind bei der Durchführung einer Hausdurchsuchung gern § 12 Abs 4 WettbG Aufsehen, Belästigungen und Störungen auf das unvermeidbare Maß zu beschränken und sind die Eigentums- und Persönlichkeitsrechte des Betroffenen soweit wie möglich zu wahren. Eine Hausdurchsuchung hat daher mit der größtmöglichen Schonung der Betroffenen durchgeführt zu werden. Auch gegen diese Verpflichtung hat die belangte Behörde gravierend verstoßen.

Die Verpflichtung zur größtmöglichen Schonung verpflichtet die belangte Behörde insbesondere auch dazu, die Hausdurchsuchung in zeitlicher Hinsicht auf das absolut erforderliche Ausmaß zu beschränken. Die Verpflichtung zur größtmöglichen Schonung korreliert diesbezüglich selbstverständlich wiederum mit dem Erfordernis, dass die gesuchten Gegenstände bereits vor dem Eingriff bestimmt sein müssen und den Betroffenen Gelegenheit gegeben wird, diese gesuchten Gegenstände herauszugeben.

Die belangte Behörde wäre daher auch aus diesem Grunde verpflichtet gewesen, die Durchführung der Hausdurchsuchung von Anbeginn an inhaltlich zu beschränken und die Dauer der Hausdurchsuchung auf das absolut erforderliche Ausmaß zu beschränken.

Wie sich jedoch bereits aus Punkt II dieser Beschwerde ergibt, hat die belangte Behörde gegen diese Grundsätze massiv verstoßen.

Zunächst ist darauf hinzuweisen, dass die belangte Behörde die Hausdurchsuchung am 20.08.2010 in der XXXX XXXX ausschließlich aufgrund der rechtsirrigen Annahme, dass die Hausdurchsuchung auf die Hauptzentrale in XXXX, "erweitert" werden könne und daher eine einheitliche Hausdurchsuchung und Maßnahme vorliegen würde, rein formal aufrecht erhalten. Dies war jedoch jedenfalls nicht erforderlich, was insbesondere durch den Umstand dokumentiert wird, dass am 20.08.2013 in der XXXX XXXX keinerlei Durchsuchungshandlungen gesetzt wurden. Trotzdem wurde die Hausdurchsuchung und sohin die Eingriffe in verfassungsgesetzlich gewährleistete Rechte von XXXX, insbesondere das Hausrecht, unnötig aufrechterhalten. Die belangte Behörde hat daher bereits aus diesem Grunde die Hausdurchsuchung in der XXXX XXXX nicht mit der größtmöglichen Schonung durchgeführt und dauerte die Hausdurchsuchung insbesondere länger, als dies zwingend erforderlich gewesen wäre. Schon daher stellt die Hausdurchsuchung in der XXXX XXXX einen Maßnahmenexzess dar. Eine Zwangsmaßnahme, die länger als unbedingt erforderlich dauert, ist stets unverhältnismäßig und damit rechtswidrig. Tatsächlich hätte die Hausdurchsuchung in der XXXX XXXX bereits am 19.08.2013 wieder beendet werden können. Die belangte Behörde hat sohin eine rechtswidrige Verzögerung der Hausdurchsuchung zu verantworten.

8.

Unzulässige Finishing Expedition

Aber auch die Durchführung der Durchsuchungshandlungen wird dem Verhältnismäßigkeitsgebot und der Verpflichtung zur größtmöglichen Schonung bei weitem nicht Gerecht, sondern stellt einen massiven Eingriff in verfassungsgesetzlich und - einfach gesetzlich gewährleistete Rechte von XXXX dar. In diesem Zusammenhang ist erneut auf die - zumindest zu Beginn der Hausdurchsuchung in XXXX - mangelnde inhaltliche Begrenzung der Durchsuchungshandlungen zu verweisen. Dies führte nicht nur dazu, dass die BWB mangels Bestimmung der gesuchten Gegenstände vor dem Eingriff eine rechtswidrige Fishing Expedition durchführte, sondern führte die mangelnde inhaltliche Begrenzung selbst auch erneut dazu, dass die Hausdurchsuchung nicht auf das unumgängliche Ausmaß eingeschränkt wurde. Dieser inhaltliche Exzess der Maßnahme war wiederum auch mit einer unnötigen Belästigung und Störung von XXXX verbunden. Es wäre im Hinblick auf den von der belangten Behörde selbst gestellten Antrag auf Anordnung einer Hausdurchsuchung und in Entsprechung des Hausdurchsuchungsbefehls angezeigt gewesen, die Hausdurchsuchung ausschließlich auf die Produktgruppen der Brauereiwirtschaft einzuschränken.

9. Unzulässige Kopie elektronischer Daten Aus den zu Punkt IV.7 dargestellten Gründen war auch die inhaltlich uneingeschränkte Kopie der gesamten Shares (Netzwerkverzeichnisse) mit der Bezeichnung ZN06-700 und ZN06-710 sowie die Kopie der gesamten Outlook-Postfächer der XXXX-Mitarbeiter /- XXXX, XXXX und XXXX im Sinne eines Maßnahmenexzesses unzulässig. Es ist bereits zu Punkt

11.7 und 11.8 dargelegt worden, dass die entsprechenden Kopien ohne jegliche inhaltliche Einschränkungen erfolgte. Darüber hinaus waren die entsprechenden elektronischen Daten physisch nicht in den Geschäftsräumlichkeiten XXXX XXXX, gespeichert. Die Kopie dieser Daten setzt daher ein Abrufen vom zentralen Server in XXXX voraus. Dies bedeutet, dass die Hausdurchsuchung vom 19.08.2013 auch in räumlicher Hinsicht den Hausdurchsuchungsbefehl überschritten hat, da dieser ausdrücklich auf die Geschäftsräumlichkeiten XXXX XXXX, beschränkt war. Es ist in diesem Zusammenhang auch klarzustellen, dass sich die Daten auf Servern, die im Eigentum der XXXXXXXX stehen, befinden. Die XXXX XXXX ist jedoch von keinem der beiden Hausdurchsuchungsbefehle umfasst. Die BWB hat ihr vom Hausdurchsuchungsbefehl klar umgrenztes Mandat sowohl in personeller als auch in örtlicher Hinsicht überschritten. Auch aus diesem Grunde liegt ein Exzess vor (vgl VfGH 01.12.2012, B619/12).

Unzulässige Weigerung, eine Versiegelung anzuerkennen

Zudem stellt die Verweigerung der von XXXX ausgesprochenen Versieglung einen weiteren Maßnahmenexzess dar. § 12 Abs 5 S 2 WettbG normiert, dass wenn ein Betroffener der Einsichtnahme in Unterlagen auf Berufung auf eine ihn treffende gesetzlich anerkannte Pflicht zur Verschwiegenheit oder ein ihm zustehendes Recht zur Verweigerung der Aussage gern § 157 Abs 1 Z 2 bis 5 StPO widerspricht, so sind diese Unterlagen auf geeignete Art und Weise gegen unbefugte Einsichtnahme oder Veränderung zu sichern und dem Kartellgericht vorzulegen. Zuvor dürfen sie nicht eingesehen werden. Das Kartellgericht hat die versiegelten Unterlagen zu sichten und mit Beschluss zu entscheiden, ob und in welchem Umfang sie eingesehen, Abschriften und Auszüge daraus angefertigt werden dürfen oder sie den Betroffenen zurückzustellen sind.

Nach dem ausdrücklichen Wortlaut bedarf eine Versieglung iSd § 12 Abs 5 WettbG keines Antrages durch den Betroffenen. Die Versiegelung erfolgt schlichtweg einfach durch den Widerspruch gegen die Prüfung von oder die Einsichtnahme in Unterlagen. Der BWB kommt sohin keine rechtliche Befugnis zu, über die Rechtmäßigkeit einer ausgesprochenen Versieglung zu entscheiden und diese anzuerkennen oder nicht. Die BWB ist vielmehr ex lege verpflichtet, ausgesprochene Versiegelungen zu akzeptieren. § 12 Abs 5 WettbG ordnet unmissverständlich an, dass die Entscheidung über die Rechtmäßigkeit der Versieglung ausschließlich dem Kartellgericht und in weiterer Folge dem Kartellobergericht obliegt.

Die Verhinderung der Versieglung unter Androhung der Anwendung behördlicher Zwangsgewalt stellt sohin jedenfalls eine Verletzung des verfassungsgesetzlich gewährleisteten Hausrechtes dar. Darüber hinaus werden dadurch auch die einfach gesetzlich gewährleisteten Rechte nach dem WettbG verletzt.

In diesem Zusammenhang ist es unerheblich, dass die Festplatte nachträglich wieder gelöscht wurde. Zum einen wurde die Löschung nicht durch Formatierung, sondern lediglich durch ein normales Löschkommando vorgenommen. Zum anderen sind die Rechtsverletzungen durch die Vornahme der Kopien und die Verhinderung der Versiegelung bereits verwirklicht worden.

Verbotener Einsatz einer Spionage-Software

Laut DUDEN (Richtiges und gutes Deutsch) ist die Spionage die Tätigkeit für einen Auftraggeber [...] zur Auskundschaftung von [...] Geheimnissen. Auskundschaften wird laut DUDEN (Das Bedeutungswörterbuch) dadurch charakterisiert, dass die Informationen heimlich in Erfahrung gebracht werden. Dementsprechend hat Trendmicro als Hersteller von Antiviren-Software von osTriage eingesetzte Programme des Herstellers als Spionage-Software klassifiziert. Der Einsatz einer Spionage-Software, wie sie die BWB bei der gegenständlichen Hausdurchsuchung einsetzte, ist per se rechtswidrig und gesetzlich nicht legitimiert. Die Befugnisse der BWB zur Einsichtnahme und Prüfung von Unterlagen im Rahmen von kartellrechtlichen Hausdurchsuchungen setzt zwingend voraus, dass diese Durchsuchungshandlungen unverdeckt erfolgen. Dies ist deshalb erforderlich, da den Betroffenen gemäß § 12 Abs 5 WettbG - wie bereits ausgeführt wurde - das Recht zukommt, bereits der Einsichtnahme zu widersprechen.

XXXX ist daher gesetzlich berechtigt, der Hausdurchsuchung beizuwohnen. Dies bedeutet nach der zutreffenden Auffassung des EGMR, dass XXXX als betroffenes Unternehmen jede Durchsuchungshandlung korrekt überwachen können muss (Urteil des EGMR vom 16.10.2007, 74336/01, Wieser/Österreich, Rn 62f; Spielmann,

Das anwaltliche Berufsgeheimnis in der Rechtsprechung des EGMR, AnwBl 2010, 346 [347]). Mit dem Einsatz einer Spionage-Software, insbesondere wenn der Einsatz verdeckt bzw ohne Information des Betroffenen erfolgt, wird dem Betroffenen jedoch gerade- die zwingende gesetzliche Möglichkeit der Überwachung der Durchsuchung und allenfalls des Widerspruchs gegen die Durchsuchung genommen.

Damit wird den Betroffenen einer Hausdurchsuchung aber auch die Möglichkeit der gesetzlich vorgesehenen Versiegelung genommen. Es handelt sich daher bei dem Einsatz der Software um nicht weniger als eine Umgehung fundamentaler Betroffenenrechte!

Für den Einsatz computerforensischer Arbeitsverfahren gibt es international anerkannte Richtlinien (Best Practices). Sogar das FBI, von dem das Programm osTriage stammt, hält sich an von der SWGDE (Scientific Working Group an Digital Evidence) erstellte Best Practices for Computer Forensics; das FBI ist selbst Mitglied dieser Arbeitsgruppe.

Alle Best Practice-Richtlinien sehen vor, dass computerforensische Arbeitsverfahren stets offen, also keinesfalls geheim, ablaufen. Dem Betroffenen sind die einzelnen Schritte zu erklären, die physikalische Umgebung der betroffenen IT und ihre Anordnung ist zu dokumentieren, eine Bestandsliste der Hardware ist zu erstellen, vom Computerforensiker ist ein entsprechender Bericht zu erstellen, in dem jeder Schritt des computerforensischen Arbeitsverfahrens der Behörde festgehalten wird, dieser Bericht ist vom Betroffenen zu unterfertigen und erhält er hievon eine Kopie.

Die BWB bzw das von ihr als Hilfskraft eingesetzte BKA hat sich an keinerlei Best Practices gehalten. Kein einziger der zuvor genannten wesentlichen Schritte im Zuge computerforensischer Arbeitsverfahren ist eingehalten worden. Der geheime Einsatz einer computerforensischen Software verstößt ganz klar gegen die berufliche Sorgfaltspflicht eines Computerforensikers und behaftet die entsprechenden Maßnahmen mit Rechtswidrigkeit.

Der Einsatz von Spionage-Software, wie sie die BWB verwendet hat, ist somit auch aus diesem Grunde a priori und jedenfalls rechtswidrig.

Nur zur Klarstellung ist auch hervorzuheben, dass der Einsatz von Spionage-Software nicht einmal im Rahmen strafgerichtlicher Ermittlungen zulässig wäre. Auch im Anwendungsbereich der StPO ist der Einsatz einer derartigen Zwangsmaßnahme nicht zulässig und existiert in Österreich daher überhaupt keine gesetzliche Grundlage für den Einsatz von Spionage-Software (Venier, Die Online-Durchsuchung. Oder: Die Freiheit der Gedanken, AnwBl 2009, 480 [480]; Reindl-Krauskopf, WK-StPO, § 134 StPO, Rn 116; Zerbes,

Das Urteil des deutschen Bundesverfassungsgerichtes zur Online-Durchsuchung und Online-Überwachung, ÖJZ 2008/89 [838]).

Die Antragsteller verkennen nicht, dass die belangte Behörde im vorliegenden Fall aufgrund des Hausdurchsuchungsbefehls zur Herstellung physischer und elektronischer Kopien berechtigt war. Diese Berechtigung umfasst schon nach ihrem Wortlaut das Herstellen von Kopien, nicht aber den Einsatz von Software zur Umgehung von Passwörtern oder zum Auslesen von WiFi-Schlüsseln.

Aber selbst wenn man annehmen wollte, dass "kopieren" gleichbedeutend mit "ausspionieren" sei (dies scheint offenbar die rechtsirrige Auslegung der BWB zu sein), erweist sich im konkreten Fall der Einsatz dieser Software als vom Wortlaut des WettbG nicht gedeckt: Zunächst hätte nämlich die Aufforderung ergehen müssen, das Gesuchte freiwillig herauszugeben, und erst dann wäre der Einsatz einer Spionagesoftware (wenn überhaupt) zulässig gewesen. Im konkreten Fall hat aber die BWB eine solche Aufforderung schlicht unterlassen (und auch nicht in ihrer Niederschrift protokolliert).

Der Einsatz der verfahrensgegenständlichen Spionage-Software ist daher a priori und per se rechtswidrig und stellt sohin an sich einen krassen Maßnahmenexzess dar.

12.

Verstöße gegen das Datenschutzgesetz Darüber hinaus wurde durch den Einsatz dieser Spionage-Software auch das Grundrecht auf Geheimhaltung gem § 1 Abs 1 DSG verletzt.

12.1

§ 1 DSG normiert als Verfassungsbestimmung das Grundrecht auf Datenschutz, wonach jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat. § 1 Abs 2 DSG erlaubt Beschränkungen des Grundrechtes auf Datenschutz bei Eingriff einer staatlichen Behörde nur aufgrund von Gesetzen, die aus den in Art 8 Abs 2 ERMK genannten Gründen notwendig sind. Derartige Gesetze müssen zur Wahrung wichtiger öffentlicher Interessen vorgesehen sein und gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen festlegen. Des Weiteren normiert § 1 Abs 2 DSG, dass auch im Falle einer zulässiger Beschränkungen der Eingriff in das Grundrecht auf Datenschutz jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf. Auch § 7 Abs 3 DSG wiederholt ausdrücklich, dass die Zulässigkeit einer Datenverwendung voraussetzt, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und dass die Grundsätze des § 6 DSG eingehalten werden.

§ 6 Abs 1 DSG legt die allgemeinen - und in einem Rechtsstaat selbstverständlichen -Grundsätze für die Verwendung von Daten fest. So dürfen Daten insbesondere nur auf rechtmäßige Weise verwendet (Z 1 leg cit), nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden (Z 2 leg cit) und ausschließlich soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen (Z 3 leg cit).

Dementsprechend dürfen Daten gemäß § 7 Abs 1 DSG nur dann verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

Sämtliche dieser Grundsätze sind von der BWB durch den Einsatz der verfahrensgegenständlichen Spionage-Software missachtet und verletzt worden.

12.2

Der Einsatz der verfahrensgegenständlichen Software durch die BWB war unter den zu Punkt IV.12.1 dargestellten Grundsätzen bereits an sich rechtswidrig.

Einleitend ist klarzustellen, dass im Rahmen einer kartellrechtlichen Hausdurchsuchung die Einsichtnahme in elektronische Dateien, also auch die Einsichtnahme in elektronische Dokumente, grundsätzlich zulässig ist (§ 12 Abs 4 iVm § 11a Abs 1 Z 2 WettbG). Voraussetzung hierfür ist jedoch - wie bereits ausgeführt wurde - dass die BWB dem Betroffenen zuvor die gesuchten Gegenstände benennt und auch tatsächlich Gelegenheit gibt, diese herauszugeben, der Betroffene die Herausgabe jedoch verweigert. Schließlich ist die Befugnis zur Einsichtnahme und daher der Datenverwendung durch den im jeweiligen Hausdurchsuchungsbefehl definierten Untersuchungsgegenstand begrenzt. Dies ergibt sich bereits aus dem in § 11 Abs 1 und § 11a Abs 1 WettbG umschriebenen allgemeinen Grundsatz, wonach die Befugnisse der BWB nur soweit reichen, als dies zur Wahrnehmung ihrer Aufgaben erforderlich ist und die erlangten Kenntnisse nur zu dem mit der Ermittlungshandlung verfolgten Zweck verwertet werden dürfen. Beide Voraussetzungen waren im gegenständlichen Fall nicht erfüllt.

Insoweit bildet der im Hausdurchsuchungsbefehl definierte Untersuchungsgegenstand (Sortimentsbereich Bier) den iSd § 6 Abs 1 Z 2 DSG festgelegen und eindeutigen Zweck der Datenverwendung und zieht zusammen mit den übrigen Bestimmungen des WettbG, insbesondere den §§ 11 bis 12 WettbG, die Grenzen der rechtlichen Befugnisse der Datenverwendung iSd § 7 Abs 1 DSG.

Auch wenn der BWB die sich auf dem USB-Stick befindlichen Programme und deren Funktionen im Detail nicht bekannt waren, so war ihr doch bewusst, dass durch den Einsatz dieser nahezu der gesamte über den jeweiligen Arbeitsplatz zugängliche Datenbestand verarbeitet und zur Abgleichung mit einer externen Datenbank übermittelt wird sowie dass Passwörter ausgelesen werden. Der BWB war es daher bewusst, dass mit dem Einsatz dieser Spionage-Software jedenfalls die Grenze des Untersuchungsgegenstandes und sohin der Zweck der Datenverwendung (§ 6 Abs 1 Z 3 DSG) massiv überschritten und im selben Ausmaß das Grundrecht auf Datenschutz verletzt wurde.

Diese Überschreitung des Untersuchungsgegenstandes und des Zweckes der Datenverwendung bedingt zugleich auch, dass die Daten, die vom Untersuchungsgegenstand nicht (mehr) umfasst sind, für den Zweck der Datenverwendung nicht wesentlich sein können. Zugleich mangelt es in diesem Ausmaß auch an einer rechtlichen Befugnis für die Datenanwendung (§ 7 Abs 1 DSG), ist diese doch ebenfalls durch den im Hausdurchsuchungsbefehl definierten Untersuchungsgegenstand begrenzt. Insoweit ist daher der Einsatz der Spionage-Software auch im Ausmaß der Überschreitung des Untersuchungsgegenstandes jedenfalls nicht erforderlich und auch nicht das gelindeste zur Verfügung stehende Mittel iSd § 7 Abs 3 DSG.

Der Eingriff in das Grundrecht auf Datenschutz durch die BWB und deren Hilfsorgane war daher bereits aus diesem Grunde jedenfalls überschießend. Diese Überlegungen gelten selbstverständlich auch hinsichtlich der uneingeschränkten Kopie der Shares mit der Bezeichnung ZN06-700 und ZN06-710 sowie der vollständigen Kopie der Mail-for Exchange-Daten der XXXX-Mitarbeiter XXXX, XXXX und XXXX.

Darüber hinaus ist die Verteidigung der belangten Behörde, die genauen Funktionen der eingesetzten Spionage-Software nicht zu kennen, nicht geeignet, die von der BWB begangenen Rechtsverletzungen, insbesondere die Verletzung des Grundrechtes auf Datenschutz, zu legitimieren. Vielmehr belegt dieses Eingeständnis eindrucksvoll den unverantwortlichen, sorglosen und damit jedenfalls unverhältnismäßigen Umgang der BWB mit den Daten der XXXX-XXXX sowie deren Mitarbeitern - rund 70.000 Mitarbeiter im In- und Ausland - sowie unzähligen GeschäftXXXXtnern. Es genügt an dieser Stelle ein Hinweis auf § 6 Abs 2 DSG, wonach der jeweilige Auftraggeber, im gegenständlichen Fall also die BWB, die Verantwortung für die Einhaltung der in § 6 Abs 1 DSG genannten Grundsätze trägt; dies selbst für den Fall, dass sich die BWB Dienstleister wie das BKA bedient. Die Verantwortung der BWB als Auftraggeber setzt geradezu voraus, dass diese über die genauen Funktionen der von ihr eingesetzten technischen Hilfsmittel wie insbesondere Software genau Bescheid weiß. Ansonsten ist die Einhaltung der Grundsätze zulässiger Datenverwendungen geradezu denkunmöglich, wie der vorliegende Fall äußerst anschaulich illustriert.

12.3

Der Einsatz der Spionage-Software war auch aus einem anderen Grunde und unabhängig von den bereits aufgezeigten Gründen nicht erforderlich und daher überschießend.

Wie bereits dargelegt wurde, war XXXX als am System angemeldeter Benutzer tätig, als ihn die BWB aufforderte, seinen Laptop zu verlassen. Der BWB und der in ihrem Auftrag agierenden Hilfskräften des BKA wurde daher der Zugang zu dem Laptop von XXXX ohne Passwortsicherung gewährt. Da die BWB als am System angemeldeter Nutzer Zugriff auf das bereits entschlüsselte Dateiensystem hatte, war der Einsatz der verfahrensgegenständlichen Software überhaupt nicht erforderlich. Der BWB war es auch ohne Einsatz der Software möglich, sämtliche vom Untersuchungsgegenstand umfassten und daher für die Untersuchung relevanten Dokumente einzusehen. Der Einsatz der Spionage-Software war daher auch aus diesem Grunde nicht erforderlich, unverhältnismäßig und überschießend.

Zu Punkt 11.6 wurde bereits dargelegt, dass das von der BWB eingesetzte Programm osTriage vom FBI entwickelt wurde und u.a. Daten automatisch mit einer Vergleichsdatenbank abgleicht. Es ist daher davon auszugehen, dass es sich um eine Vergleichsdatenbank des FBI handelt und diese daher in den USA situiert ist. Dass ein entsprechender Datenvergleich und sohin eine Übermittlung oder Überlassung von Daten stattgefunden hat, wurde von der BWB auch gar nicht bestritten.

Gemäß § 4 Z 8 DSG ist unter Verwenden von Daten jede Art der Handhabung, inklusive das Übermitteln zu subsumieren. Die Verwendung von Daten setzt als Grundbedingung voraus, dass die Daten aus einer nach § 7 Abs 1 DSG zulässigen Anwendung stammen. Dass dies gerade nicht der Fall war, wurde bereits ausführlich dargelegt. Die Übermittlung der Daten im Wege des automatischen Datenabgleiches mit einer Vergleichsdatenbank ist daher bereits aus diesem Grunde unzulässig und verletzt das Grundrecht auf Datenschutz. Dies insbesondere auch vor dem Hintergrund, dass das WettbG der BWB gerade keine rechtliche Befugnis verleiht, Daten an Dritte, mit Ausnahme des Kartellgerichtes, zu übermitteln.

Darüber hinaus ist eine Übermittlung oder Überlassung von Daten in die USA nur dann genehmigungsfrei möglich, wenn der Empfänger der sogenannten "Safe Harbor"Regelung beigetreten ist (§ 1 Abs 1 Z 1 DSAV iVm § 12 Abs 2 DSG). Das FBI ist dem Safe Harbor jedoch nicht beigetreten, weshalb die Voraussetzungen für eine genehmigungsfreie Übermittlung oder Überlassung nicht vorliegen. Klarstellend ist festzuhalten, dass auch die Voraussetzungen des § 12 Abs 3 DSG nicht erfüllt sind. Die BWB hätte daher vor der Übermittlung der Daten gemäß § 13 Abs 1 DSG eine Genehmigung der Datenschutzkommission (im Folgenden auch kurz als "DSK" bezeichnet") einholen müssen.

Da die BWB Daten ohne Einholung der vorherigen Genehmigung durch die DSK und obwohl die Voraussetzungen des § 12 Abs 2 oder Abs 3 DSG nicht vorlagen, in die USA und sohin einen Drittstaat übermittelte, hat sie auch aus diesem Grunde das Grundrecht auf Datenschutz verletzt.

13.

Unterbliebene Zeugenbelehrungen Gemäß § 12 Abs 4 WettbG kommen der belangten Behörde bei Hausdurchsuchungen die in § 11a Abs 1 Z 2 und 3 WettbG genannten Befugnisse zu. § 11a Abs 1 Z 3 WettbG räumt der belangten Behörde die Befugnis ein, vor Ort alle für die Durchführung von Ermittlungshandlungen erforderlichen Auskünfte zu verlangen sowie von allen Vertretern oder Beschäftigten des Unternehmens Erläuterungen zu Sachverhalten oder Unterlagen zu verlangen, die mit Gegenstand und Zweck der Ermittlungen im Zusammenhang stehen. Abs 2 leg cit bestimmt jedoch, dass ausschließlich der Inhaber des Unternehmens sowie bei juristischen Personen die nach Gesetz oder gesetzlichen Vertreter zur Vertretung berufenen Personen, sohin die organschaftlichen Vertreter, verpflichtet sind, die verlangten Auskünfte nach Abs 1 Z 3 leg cit zu erteilen.

Im Rahmen von Hausdurchsuchungen sind daher Beschäftigte des betroffenen Unternehmens nicht verpflichtet, Auskünfte zu erteilen (vgl Kaps, KaWeRÄG 2012: Auskunftsverlangen und Versiegelung - alles neu? wbl 2013, 369 [370]).

Gemäß § 11 Abs 2 WettbG sind unter anderem die §§ 46 bis 51 AVG anzuwenden. Gemäß § 50 AVG ist jeder Zeuge zu Beginn seiner Vernehmung auf die gesetzlichen Gründen für die Verweigerung der Aussage aufmerksam zu machen.

§ 11 a WettbG stellt im Verhältnis zu den § 48 und 49 AVG eine leg specialis dar und

erweitert sohin diese Bestimmungen. Da § 11 a Abs 2 WettbG die Aussagepflicht ausdrücklich auf den Unternehmer bzw die organschaftlichen Vertreter einschränkt, besteht daher hinsichtlich der übrigen Beschäftigten keine Pflicht zur Aussage. Mangels Pflicht zur Aussage sind diese jedoch zumindest berechtigt, die Aussage zu verweigern. Dies erfordert jedoch, dass die Zeugen gemäß § 50 AVG ausdrücklich über ihr Recht, die Aussage zu verweigern, belehrt werden müssen (vgl Kirchbacher, WK-StPO, § 156, Rn 2)

Die belangte Behörde hat es jedoch unterlassen, die einvernommenen Zeugen darüber aufzuklären, dass diese berechtigt sind, die Aussage zu verweigern. Auch dies stellt eine schwerwiegende Rechtsverletzung und sohin einen Maßnahmenexzess dar.

Maßnahmenexzess in XXXX am 20.08.2013

Die Unverhältnismäßigkeit und somit Unzulässigkeit der Hausdurchsuchung wird auch dadurch verwirklicht, dass die belangte Behörde ausschließlich nach einem einzigen Dokument gesucht hat, welches sie bereits bei XXXX in XXXX gefunden und unversiegelt zum Akt genommen hat; darüber hinaus war der BWB dieses Dokument auch schon vor der Hausdurchsuchung in XXXX bekannt, weil es sich um eine Beilage zum Antrag auf Bewilligung der Hausdurchsuchung gehandelt hatte. Ein zusätzlicher Erkenntnisgewinn ist daher ausgeschlossen. Die Hausdurchsuchung war daher auch aus diesem Grunde gar nicht a priori erforderlich. Schließlich ist die Durchführung einer Hausdurchsuchung zur Erlangung eines einzigen Dokumentes per se unverhältnismäßig und auch aus diesem Grunde rechtswidrig. Vielmehr hätte die BWB das gelindere Mittel des Auskunftsverlangens nach § 11 a Abs 1 Z 1 WettbG anwenden müssen. Auch hätte XXXX das gesuchte Dokument auf Nachfragen jedenfalls freiwillig herausgegeben. Dies ist bereits durch den Umstand dokumentiert, dass es bereits unversiegelt Bestandteil des Ermittlungsaktes der BWB wurde.

In diesem Zusammenhang ist auch auf das Argument der belangten Behörde, sie wollte überprüfen, ob sich in den Outlook-Postfächern dieselben Dokumente befinden, wenn sie auf diese aus der HZ zugreift, zu verweisen. Dies ist bereits technisch bedingt; es ist vollkommen irrelevant, von welchem Ort man auf ein Outlook-Postfach zugreift. Auch aus diesem Grunde war die Hausdurchsuchung jedenfalls nicht erforderlich und stellt somit einen Eingriff in das verfassungsgesetzlich gewährleistete Hausrecht dar.

Gesamte Hausdurchsuchungen rechtswidrig

Beschwerden gegen die Ausübung unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt gem § 67a Z 2 AVG haben nach § 67c Abs 2 Z 5 leg cit das Begehren zu enthalten, den angefochtenen Verwaltungsakt für rechtswidrig zu erklären. Der angefochtene Verwaltungsakt ist die durch die BWB am 19.08.2013 in der Zweigniederlassung von XXXX in XXXX und am 20.08.2013 gleichfalls dort und in der Hauptzentrale in XXXX durchgeführte Hausdurchsuchung. Nach Ansicht der Beschwerdeführer ist der Gesetzeswortlaut insofern eindeutig, als bei Feststellen auch nur eines Maßnahmenexzesses der gesamte angefochtene Verwaltungsakt zwingend für rechtswidrig zu erklären ist. Die Rechtsansicht der Beschwerdeführer wird noch dadurch erhärtet, dass die belangte Behörde über den Verwaltungsakt ein Protokoll geführt hat, in dem einerseits der Beginn des Verwaltungsaktes, nämlich der Hausdurchsuchung, und das Ende dieses einen Verwaltungsaktes festgehalten wurde."

Mit Schreiben an den UVS Salzburg vom 30.09.2013 erhoben die Beschwerdeführerinnen eine Maßnahmenbeschwerde gegen die Hausdurchsuchung vom 20.08.2013 in XXXX, worin sie zum Sachverhalt und den Beschwerdegründen entsprechend ähnliches wie zu der Hausdurchsuchung in XXXX, vorbringt.

Mit 2 Schreiben vom 22.11.2013 erstattete die BWB zwei Gegenschriften.

Mit Schreiben der Beschwerdeführerinnen vom 9.1.2014 erwiderten diese dem Vorbringen der belangten Behörde in der Gegenschrift und legten eine gutachterliche Stellungnahme von Professor Dr. XXXX vom 8.10.2013 vor. Diese bezieht sich auf die gegenständliche Hausdurchsuchung und führt unter Punkt 3.2.1 Grundlagen wie folgt aus: "Bei einer Hausdurchsuchung hat die BWB das Recht,

- die geschäftlichen Unterlagen zu sichten ("einzusehen", § 11a Abs. 1 Z 2 iVm § 12 Abs. 4 WettbG)

- die geschäftlichen Unterlagen zu kopieren ("Abschriften und Auszüge der Unterlagen anzufertigen" § 11a Abs. 1 Z 2 iVm § 12 Abs. 4 WettbG)

- Beweismittel in ihre Verfügungsmacht zu bringen ("Beweismittel in Beschlag zu nehmen" § 12 Abs. 4 WettbG)

Diese Zugriffsrechte beziehen sich auf die geschäftlichen Unterlagen "unabhängig davon, in welcher Form sie vorliegen": auch elektronisch gespeicherte Unterlagen sind damit erfasst. Es kommt auch nicht darauf an, ob diese Unterlagen auf der Festplatte eines in den durchsuchten Räumlichkeiten befindlichen Endgeräts gespeichert werden oder ob diese Unterlagen auf externen Speicherplätzen liegen."

Mit Schreiben der BWB vom 15.4.2014 wurde eine weitere Gegenschrift samt Beilagen vorgelegt, welche allesamt nicht entscheidungsrelevant sind.

Mit Schreiben der BWB vom 12. September 2014 wurde der Beschluss des Obersten Gerichtshofes als Kartellobergericht vom 14. Februar 2014 vorgelegt.

Die mündliche Verhandlung fand am 16. September 2014 im Bundesverwaltungsgericht statt.

II. Das Bundesverwaltungsgericht hat erwogen:

1. Feststellungen:

Mit Beschluss vom 6.8.2013, 26 Kt 88/13-2, ordnete das Oberlandesgericht Wien als Kartellgericht über Antrag der BWB wegen des begründeten Verdachts der Teilnahme an wettbewerbswidrigen Vereinbarungen und/oder abgestimmten Verhaltensweisen und zwar betreffend vertikale Preisabstimmungen der Erstbeschwerdeführerin mit Unternehmen der Brauereiwirtschaft sowie horizontale Preisabstimmungen des Einzelhandels über Unternehmen der Brauereiwirtschaft in den Geschäftsräumlichkeiten und Fahrzeugen der Erstbeschwerdeführerin am Standort XXXX XXXX, und die Sicherstellung von physischen und elektronischen Kopien an. Mit der Durchführung der Hausdurchsuchung und der Zustellung dieser Entscheidung an das betroffene Unternehmen wurde die BWB beauftragt. In der rechtlichen Beurteilung dieses Beschlusses wurde darauf hingewiesen, dass auch nach Informationsquellen gesucht werden darf, die noch nicht bekannt sind und dass für die Zweckmäßigkeit einer Hausdurchsuchung insbesondere eine Verdunkelungsgefahr spricht. (Beschluss des Oberlandesgericht Wien vom 6.8.2013, 26 Kt 88/13-2)

Mit Beschluss vom 20.8.2013, 26 Kt 88/13-4, 26 Kt 101/13, 102/13, erweiterte das Oberlandesgericht Wien als Kartellgericht den oben genannten Hausdurchsuchungsbefehl vom 6.8.2013 auf die Geschäftsräumlichkeiten der Erstbeschwerdeführerin, Zweitbeschwerdeführerin und Drittbeschwerdeführerin jeweils in XXXX. (Beschluss des Oberlandesgericht Wien vom 20.8.2013, 26 Kt 88/13-4, 26 Kt 101/13, 102/13)

Sowohl der Beschluss vom 6.8.2013, 26 Kt 88/13-2, als auch der Beschluss vom 20.8.2013, 26 Kt 88/13-4, 26 Kt 101/13, 102/13, wurden von den Beschwerdeführerinnen mit Rekurs bekämpft. Mit Beschluss des Obersten Gerichtshofes als Kartellobergericht vom 14. Februar 2014, 16 Ok 8/13, 16 Ok 9/13, wurde beiden Rekursen nicht Folge gegeben. (Beschluss des Obersten Gerichtshofes als Kartellobergericht vom 14. Februar 2014, 16 Ok 8/13, 16 Ok 9/13)

Die Hausdurchsuchung fand am 19. August 2013 in XXXX, und am 20. August 2013 in XXXX sowie in XXXX, statt.

XXXX und XXXX, beide Bedienstete des Bundeskriminalamtes (BKA) und zuständig für die IT-Beweissicherung und IT-Forensik, waren am 19.08.2013 bei der Hausdurchsuchung der XXXX XXXX (XXXX) für die Bundeswettbewerbsbehörde (BWB) als Assistenten tätig. Sie sollten helfen, den durch den Hausdurchsuchungsbefehl vorgegebenen gerichtlichen Auftrag umzusetzen, indem sie aufgrund ihrer besonderen IT-Fachkenntnis unterstützend tätig werden. Bei Zustellung des Hausdurchsuchungsbefehls gab es eine Besprechung zwischen XXXX, BWB und BKA Mitarbeitern. XXXX gab ihnen den Auftrag, die Rechner von XXXX/XXXX und XXXX/XXXX in Hinblick auf versteckte Dateien, die Bierabsprachen betreffen, zu durchsuchen. (Protokoll der mündlichen Verhandlung vom 16. September 2014, S. 5)

In der Folge sind XXXX und XXXX zum Arbeitsplatz von Herrn XXXX gegangen, dieser war in einem Großraumbüro. Eine Mitarbeiterin der BWB, Mag. XXXX, ist auf dem Sessel vor dem Laptop von XXXX gesessen, um sie herum standen Herr XXXX, ein Protokollist der XXXX, ein Protokollist der BWB, sowie ein Rechtsvertreter der XXXX. Mag. XXXX hat in der Folge den Laptop in herkömmlicher Art und Weise, unter Verwendung des am Computer bereits installierten Windows-Explorers, durchsucht. XXXX und XXXX haben dabei Mag. XXXX "über die Schulter geschaut". XXXX ist in der Folge aufgefallen, dass eine BITLOCKER-Verschlüsselung auf dem Notebook eingeschaltet war. Das Programm des BITLOCKERS bewirkt eine Verschlüsselung der Dateien auf Hardwareebene beziehungsweise der kompletten Festplatte, wobei die Daten im Normalfall für den Anwender zugänglich sind, außer dieser Zugang wird blockiert, sei es vom Administrator

über das Netzwerk, durch das Zuklappen des Notebooks, durch Stromverlust, oder durch Herunterfahren des Computers und so weiter. Mittels Fernzugriff ist es ohne weiteres möglich, die Verschlüsselung zu aktivieren, oder Daten zu löschen. Da eine aktive Netzwerkverbindung zwischen dem Server in der Zentrale in XXXX und in XXXX bestanden hat, wäre es möglich gewesen, Daten von XXXX aus in der Zweigniederlassung in XXXX zu löschen beziehungsweise zu manipulieren. Um zu verhindern, dass das BITLOCKER-Programm die Daten verschlüsselt und damit für die belangte Behörde unleserlich macht, haben XXXX und XXXX als Vorsichtsmaßnahme beschlossen, mit Hilfe des Einsatzes des forensischen Programms DumpIT den Arbeitsspeicher des durchsuchten Notebooks zu sichern, weil in diesem Arbeitsspeicher der Schlüssel für das kryptografische Programm BITLOCKER abgelegt ist. Auf diese Weise wären sie in der Lage, auch eine Kopie der Festplatte, die mit dem BITLOCKER-Programm verschlüsselt ist, zu entschlüsseln. XXXX hat in der Folge Frau Mag. XXXX auf das Problem des BITLOCKER-Programmes aufmerksam gemacht, woraufhin sie den Arbeitsplatz für XXXX geräumt hat und er sich auf diesen Arbeitsplatz setzte. Die oben genannten anwesenden Personen haben diesen Vorgang gesehen. (Protokoll der mündlichen Verhandlung vom 16. September 2014, S. 6)

Die XXXX XXXX hat sich gegenüber XXXX nicht kooperativ verhalten und das Administratorenpasswort nicht herausgegeben. (Protokoll der mündlichen Verhandlung vom 16. September 2014, S. 8)

XXXX hat in der Folge den forensischen USB-Stick am Laptop von Herrn

XXXX angesteckt und vorerst nur versucht, das Programm DumpIT auszuführen. Die Ausführung des Programmes DumpIT hat jedoch aufgrund mangelnder Benutzerrechte nicht funktioniert. Das Programm hat sich nicht starten lassen. Die Ausführung des Programmes DumpIT ist somit fehlgeschlagen. In der Folge wollten sich XXXX und XXXX einen Überblick über das Notebook verschaffen, das heißt, in Erfahrung bringen, an welche Netzlaufwerke das Notebook angeschlossen ist, eine Übersicht des verwendeten Betriebssystems, des angemeldeten Benutzers, ob ein versteckter und/oder verschlüsselter Container (eine versteckte oder nicht versteckte Datei, die verschlüsselte oder nichtverschlüsselte Dateien enthält) vorhanden ist, generell die verwendeten Festplatten - physikalisch und logisch (logische Festplatten sind Partitionen bei physikalischen Festplatten), ob ein verschlüsselter Container geöffnet und damit zugänglich ist. Um diesen Überblick zu bekommen, wurde speziell für diesen Zweck das Programm osTRIAGE von XXXX und XXXX verwendet. OsTRIAGE wird von ungefähr 50 Behörden weltweit eingesetzt. Dazu hat XXXX das Programm osTRIAGE vom USB-Stick aus versucht zu starten. Programme wurden auf dem Computer keinesfalls installiert, weil das ein forensischer Grundsatz ist. Der vorhandene Virenscanner hat beim Programm osTRIAGE angeschlagen und hat eine Meldung auf dem Bildschirm sichtbar gemacht. Das ist von XXXX und XXXX bewusst ignoriert worden. Normalerweise muss man vor dem Starten des Programmes osTRIAGE die Antivirensoftware deaktivieren, um solche Meldungen, die false positives heißen, zu verhindern. In der Folge ist auf dem Computer nichts passiert. Im Normalfall sollte nach Starten des Programmes osTRIAGE folgendes passieren: Es öffnet sich ein Fenster, auf dem das Logo von osTRIAGE ersichtlich ist und ein Ladebalken, kurz darauf ein weiteres Fenster mit einem großen Stoppschild. Dieses Prozedere dauert im Normalfall nicht länger als ein paar Minuten. Dieses normale Prozedere ist nicht passiert und daher haben XXXX und XXXX den Taskmanager geöffnet, um zu sehen, ob der Prozess osTRIAGE läuft. Im Taskmanager haben XXXX und XXXX den Eintrag bei Anwendungen oder Prozesse von osTRIAGE gesehen, wobei die Meldung "reagiert nicht" oder ähnliches vermerkt war, woraus

XXXX und XXXX geschlossen haben, dass das Programm nicht ordnungsgemäß gelaufen ist. In der Folge hat XXXX den Prozess osTRIAGE beendet. (Protokoll der mündlichen Verhandlung vom 16. September 2014, S. 7, 9)

XXXX hat anschließend das auf dem Rechner befindliche Programm Snipping-Tool geöffnet und damit zwei Screenshots angefertigt. Weitere Handlungen haben XXXX und XXXX auf diesem Computer nicht durchgeführt. Auf dem Computer von Frau XXXX haben XXXX und XXXX keine forensische Software ausgeführt, sondern lediglich zwei Screenshots ebenfalls mit dem Programm Snipping-Tool angefertigt. Weitere Handlungen auf Computern der XXXX haben XXXX und XXXX nicht durchgeführt. Die Tätigkeit am Computer des Herrn XXXX hat ca. 20-30 Minuten gedauert. XXXX und XXXX waren dann noch ein paar Minuten vor Ort und wurden um die Mittagszeit entlassen. XXXX und XXXX haben keine Daten kopiert; osTRIAGE selbst kopiert auch keine Daten sondern ist beim Auffinden von Daten behilflich. Wenn Daten kopiert werden sollen, muss dies der Anwender selbst durchführen. Ein Logfile (Protokoll über die Aktivitäten des Programms) wurde von osTRIAGE nicht angelegt, weil das Programm nicht korrekt zur Anwendung gekommen ist. (Protokoll der mündlichen Verhandlung vom 16. September 2014, S. 7f)

XXXX ist Informatiker und hatte beim BKA die Aufgabe als Amtssachverständiger im Bereich Informatik im Cyber Crime Competence Center des BKA tätig zu werden. Er war zuständig zur Überprüfung und Zertifizierung von Software, Programmanalyse und die Erarbeitung von internationalen Normen im Bereich IT-Forensik, weiters war er zuständig für die Sicherstellung der Einhaltung von internationalen Normen im Bereich IT-Forensik. XXXX war mit der Hausdurchsuchung nicht unmittelbar befasst. Er ist nach der Hausdurchsuchung

hinzugezogen worden, nachdem sich Fragen oder Probleme mit der XXXX ergeben haben. Seine Aufgabe war das Überprüfen der Vorhaltungen und Befürchtungen seitens der XXXX aber auch das Überprüfen der Behauptungen der Beamten des BKA. XXXX hat die verwendeten Werkzeuge und den eingesetzten USB-Stick (Datenträger) einer Prüfung unterzogen sowie die beiden Beamten befragt bzw. ebenfalls einer Prüfung unterzogen. Zusammengefasst ergibt sich folgendes Bild betreffend den von XXXX untersuchten USB-Stick: Bei der Hausdurchsuchung sind vom Bundeskriminalamt-Stick zwei Programme manuell gestartet worden. Das erste war DumpIT, dieses Programm dient der Sicherung des Zugangs zum gegenständlichen Computer, das zweite Programm war osTRIAGE. Dieses Programm wird im Bundeskriminalamt eingesetzt, um zeitnahe eine Übersicht über den Datenbestand am Gerät zu erhalten. Für die erfolgreiche Ausführung von DumpIT waren zu geringe Benutzerrechte vorhanden. DumpIT hat daher keine Zugangsschlüssel sichern können. Die Ausführung von osTRIAGE wurde vom Sicherheitssystem der XXXX IT als konzernfremde Software identifiziert, als Sicherheitsrisiko eingestuft und an der Ausführung gehindert. Beide Programme sind daher nicht zur erfolgreichen Ausführung gekommen, mit beiden Programmen wurden keine Daten erfasst und aufgezeichnet. Da diese beiden Programme die gelindesten Mittel für eine Datensicherung seitens des BKA darstellt, konnte der erteilte Sicherungsauftrag nicht ausgeführt werden. Vom Einsatz stärkerer Programme, die einen Zugriff ermöglicht hätten, wurde Abstand genommen, um eine etwaige Schädigung des XXXX IT-Systems zu vermeiden. OsTRIAGE erzeugt forensische Protokolldateien (Logfiles), bei erfolgreichem Durchlauf jeder Teilaufgabe. Da osTRIAGE aber im Ansatz beendet wurde, wurden keine Logfiles erzeugt. Der gegenständliche USB-Stick ist nach der Hausdurchsuchung im Bundeskriminalamt forensisch von XXXX untersucht worden. Die Untersuchung hat ergeben, dass, wie von den Beamten des Bundeskriminalamtes behauptet, keine Logfiles am Stick gespeichert wurden. Der Stick enthielt neben den standardmäßig enthaltenen Werkzeugen des Bundeskriminalamtes vier Screenshots, die von den Beamten während der Hausdurchsuchung zu Dokumentationszwecken angefertigt wurden. Ansonsten enthielt der Stick keine weiteren, während der Hausdurchsuchung erzeugten Dateien. (Protokoll der mündlichen Verhandlung vom 16. September 2014, S. 17)

Es gibt zwei Gründe warum man die Programme DumpIT und osTRIAGE einsetzt. Zum Einen kann der Betroffene ja lügen und zum Anderen könnte das Gerät auch über das Netzwerk von außen manipuliert werden. Der Einsatz von DumpIT verhindert zudem den Verlust des Zugriffs auf die Daten im Fall eines Stromausfalls, weil dort der Zugriffsschlüssel verloren ginge. Der Einsatz von osTRIAGE in der Funktion als erzeugendes Werkzeug für eine "Überblickskarte", also einen Überblick über den Speicherort der Daten, beschleunigt die Amtshandlung um ein Vielfaches, gegenüber einer reinen manuellen Sicht. (Protokoll der mündlichen Verhandlung vom 16. September 2014, S. 18)

2. Beweiswürdigung:

Der festgestellte Sachverhalt ergibt sich schlüssig aus den jeweils in Klammern genannten unbedenklichen Quellen.

Bei der mündlichen Verhandlung waren die Aussagen der Zeugen XXXX, XXXX und XXXX widerspruchsfrei, schlüssig und insgesamt als glaubhaft zu erachten. Alle drei genannten Zeugen hinterließen den Eindruck, dass sie bestrebt waren, offen und bereitwillig bei der Wahrheitsfindung mitzuwirken. Auch der persönliche Gesamteindruck der drei genannten Zeugen in der Verhandlung war der von zuverlässigen und glaubwürdigen Beamten.

Wesentlich zur Feststellung des Sachverhaltes beigetragen haben insbesondere die Zeugen XXXX und XXXX, welche direkt vor Ort bei der Hausdurchsuchung durchführend tätig waren. Die Aussagen des Zeugen XXXX, der nicht direkt vor Ort bei der Hausdurchsuchung durchführend tätig war, dienten lediglich der Abrundung und Bestätigung des bereits durch XXXX und XXXX geprägten Bildes sowie der Erlangung von allgemeinen Hintergrundinformationen.

3. Rechtliche Beurteilung:

3. a) Grundsätzliche rechtliche Erwägungen

Gemäß Art. 130 Abs. 1 Z 2 B-VG erkennen die Verwaltungsgerichte über Beschwerden gegen die Ausübung unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt wegen Rechtswidrigkeit. Da es sich in den gegenständlichen Rechtssachen um eine Angelegenheit der Vollziehung des Bundes, die unmittelbar von Bundesbehörden besorgt wird handelt, sind nunmehr nicht mehr der UVS Kärnten und der UVS Salzburg sondern das Bundesverwaltungsgericht für die Entscheidung über die gegenständlichen Maßnahmenbeschwerden zuständig.

Der VwGH führt in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005 ua., aus (Hervorhebungen durch das BVwG):

"Werden solche behördlichen Akte in Durchführung richterlicher Befehle gesetzt, fallen sie nicht in den Bereich der Hoheitsverwaltung, sondern sie sind - solange die Verwaltungsorgane den ihnen durch den richterlichen Befehl gestellten Ermächtigungsrahmen nicht überschreiten - funktionell der Gerichtsbarkeit zuzurechnen. Bei offenkundiger Überschreitung des richterlichen Befehls liegt hingegen insoweit ein der Verwaltung zuzurechnendes Organhandeln vor (vgl. etwa die hg. Erkenntnisse vom 23. September 1998, Zl. 97/01/1084, 1085 und 1087, vom 6. Juli 1999, Zl. 96/01/0061, 0062, vom 20. Juni 2008, Zl. 2007/01/1166, und vom 7. Oktober 2010, Zl. 2008/17/0222; vgl. weiters etwa VfGH vom 17. Juni 1991, B 1017/90, mwN und vom 20. September 2012, B 1233/11).

Dabei kommt es entscheidend darauf an, ob die gesetzten Maßnahmen durch die gerichtliche Anordnung gedeckt waren. Ausgangspunkt einer entsprechenden Beurteilung ist der Wortlaut des richterlichen Befehls (vgl. etwa das hg. Erkenntnis vom 24. August 2004, Zl. 2003/01/0041). Auch dessen Sinngehalt ist für die Auslegung von Bedeutung (vgl. etwa VfGH vom 17. Juni 1991, B 1017/90).

Die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt wird nicht schon dadurch unterbrochen, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen. Durchbrochen wird der Auftragszusammenhang des Organhandelns zur richterlichen Gewalt nur durch solche Maßnahmen, die ihrem Inhalt und Umfang nach in der gerichtlichen Anordnung keine Deckung mehr finden. Eine Hausdurchsuchung auf Grund gerichtlicher Anordnung bleibt somit gleichwohl der Akt eines Gerichtes und ist deshalb der Überprüfung durch die unabhängigen Verwaltungssenate entzogen, wenn bei Durchführung der gerichtlichen Anordnung eine Gesetzwidrigkeit (z.B. die unterlassene Zustellung des Hausdurchsuchungsbefehls oder die unterlassene Befragung des Betroffenen vor Beginn der Hausdurchsuchung) unterläuft. Die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, sind keine vor den unabhängigen Verwaltungssenaten selbständig bekämpfbaren Maßnahmen. Bei einer auf Grund eines richterlichen Befehls durchgeführten Hausdurchsuchung ist auch die Vorgangsweise bei Durchsetzung des Hausdurchsuchungsbefehls dem Gericht zuzurechnen (vgl. etwa die hg. Erkenntnisse vom 23. September 1998, Zlen. 97/01/1084, 1085 und 1087, vom 6. Juli 1999, Zl. 96/01/0061, 0062, vom 16. Februar 2000, Zl. 96/01/0233, vom 17. Mai 1995, Zl. 94/01/0763; ebenso VfGH vom 30. September 1991, B 1108/90, und vom 26. September 1988, B 608/87, u.a.).

Diese Grundsätze gelten - wie im Hinblick auf den Beschluss des Obersten Gerichtshofes (OGH) vom 6. Juni 2012, 16 Ok 2/12, festzuhalten ist - auch für Hausdurchsuchungen nach § 12 WettbG. Dementsprechend kommt eine Überprüfung der Vorgangsweise der Bundeswettbewerbsbehörde anlässlich einer gerichtlich angeordneten Hausdurchsuchung durch die unabhängigen Verwaltungssenate auch in diesen Fällen nur in Betracht, soweit es zu einer offenkundigen Überschreitung des richterlichen Befehls ("Exzess") gekommen ist (vgl. in diesem Sinn bereits das in der gegenständlichen Angelegenheit ergangene Erkenntnis des VfGH vom 1. Dezember 2012, B 619/12-10, mwN, wonach eine Rechtsschutzlücke nicht zu erkennen ist)."

Der gegenständliche Hausdurchsuchungsbefehl vom 6.8.2013 erweitert am 20.8.2013 ordnet (verkürzt dargestellt) wegen des begründeten Verdachts der Teilnahme an wettbewerbswidrigen Vereinbarungen im Bereich der Brauereiwirtschaft vorerst in den Geschäftsräumlichkeiten und Fahrzeugen der Erstbeschwerdeführerin am Standort XXXX XXXX, und schließlich erweitert auf die Geschäftsräumlichkeiten der Erst- bis Drittbeschwerdeführerinnen auch in XXXX, die Sicherstellung von physischen und elektronischen Kopien an. Wie dem Hausdurchsuchungsbefehl vom 6.8.2013 in der rechtlichen Beurteilung zu entnehmen ist, bestand Verdunkelungsgefahr und des durfte auch nach Informationsquellen gesucht werden, die noch nicht bekannt sind.

Bei der Hausdurchsuchung hatte die BWB somit - worauf die Beschwerdeführerinnen durch Vorlage der gutachterlichen Stellungnahme von Professor Dr. XXXX vom 8.10.2013 zu Recht verweisen - das Recht,

- die geschäftlichen Unterlagen zu sichten ("einzusehen", § 11a Abs. 1 Z 2 iVm § 12 Abs. 4 WettbG)

- die geschäftlichen Unterlagen zu kopieren ("Abschriften und Auszüge der Unterlagen anzufertigen" § 11a Abs. 1 Z 2 iVm § 12 Abs. 4 WettbG)

- Beweismittel in ihre Verfügungsmacht zu bringen ("Beweismittel in Beschlag zu nehmen" § 12 Abs. 4 WettbG).

Diese Zugriffsrechte beziehen sich auf die geschäftlichen Unterlagen "unabhängig davon, in welcher Form sie vorliegen": Auch elektronisch gespeicherte Unterlagen sind damit erfasst. Es kommt auch nicht darauf an, ob diese Unterlagen auf der Festplatte eines in den durchsuchten Räumlichkeiten befindlichen Endgeräts gespeichert werden oder ob diese Unterlagen auf externen Speicherplätzen liegen.

Gemäß § 14 Abs. 2 WettbG sind im Rahmen einer Hausdurchsuchung der BWB die hilfeleistenden Organe des öffentlichen Sicherheitsdienstes auch ermächtigt, die BWB durch die Sicherung von Unterlagen in elektronischer Form zu unterstützen. Gemäß § 12 Abs. 4 WettbG sind bei der Durchführung der Hausdurchsuchung Aufsehen, Belästigungen und Störungen auf das unvermeidbare Maß zu beschränken. In diesem Sinne ist es zulässig, wenn die BWB bei einer Hausdurchsuchung forensische Computerprogramme verwendet, um dem Zweck der Amtshandlung, nämlich eine große Datenmenge schnell und effizient sichten zu können, zum Durchbruch zu verhelfen. Weiters ist es zulässig, wenn die BWB bei einer Hausdurchsuchung forensische Computerprogramme verwendet, um dem Zweck der Amtshandlung, nämlich geschäftliche Unterlagen zu kopieren und diese in einer für sie lesbaren Form (also nicht etwa verschlüsselt) in ihre Verfügungsmacht zu bringen, zum Durchbruch zu verhelfen. Gemäß § 12 Abs. 4 WettbG sind die Eigentums- und Persönlichkeitsrechte desjenigen, bei dem die Hausdurchsuchung vorgenommen wird (Betroffener), soweit wie möglich zu wahren. Bei der Verwendung von forensischen Computerprogrammen bei einer Hausdurchsuchung durch die BWB hat diese somit darauf zu achten, Beschädigungen am Eigentum und Eingriffe in die Persönlichkeitsrechte der Betroffenen soweit wie möglich hintanzuhalten.

3. b) Zu der behaupteten Rechtswidrigkeit "3. Rekurse gegen Hausdurchsuchungsbefehle"

Da den Rekursen gegen den Hausdurchsuchungsbefehl mit Beschluss des Obersten Gerichtshofes als Kartellobergericht vom 14. Februar 2014, 16 Ok 8/13, 16 Ok 9/13, nicht Folge gegeben wurde, erübrigt sich ein weiteres Eingehen auf diesen Punkt.

3. c) Zu der behaupteten Rechtswidrigkeit "4. Verspätete Zustellung des Hausdurchsuchungsbefehls vom 06.08.2013"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Eine etwaige verspätete Zustellung des Hausdurchsuchungsbefehls vom 6.8.2013 stellt daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar.

3. d) Zu der behaupteten Rechtswidrigkeit "5. Keine Prüfungsmöglichkeit durch XXXX"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Eine etwaige unterlassene Prüfungsmöglichkeit stellt daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar.

3. e) Zu den behaupteten Rechtswidrigkeiten "6. Verstoß gegen § 12 Abs 5 WettbG" und "8. Unzulässige Fishing Expedition"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns

zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Eine etwaiges Unterlassen vor der verfahrensgegenständlichen Hausdurchsuchung die Beschwerdeführerinnen hinsichtlich der Voraussetzungen der Hausdurchsuchung zu befragen und sie aufzufordern und ihnen Gelegenheit zu geben, die gesuchten Gegenstände freiwillig herauszugeben, stellt daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar. Im Übrigen wird darauf hingewiesen, dass in der rechtlichen Beurteilung des Beschlusses des Oberlandesgerichts Wien vom 6.8.2013, 26 Kt 88/13-2 darauf hingewiesen wurde, dass auch nach Informationsquellen gesucht werden darf, die noch nicht bekannt sind. Ein Exzess durch eine "unzulässige Fishing Expedition" liegt daher jedenfalls nicht vor.

3. f) Zu der behaupteten Rechtswidrigkeit "7. Zeitlicher Exzess der Hausdurchsuchung in XXXX"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Im Übrigen hat die belangte Behörde versucht, bei der Hausdurchsuchung forensische Computerprogramme zu verwenden, um eine große Datenmenge schnell und effizient sichten zu können, war also grundsätzlich bestrebt, Störungen auf das unvermeidbare Maß zu beschränken. Das gerügte Verhalten der belangten Behörde stellt daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar.

3. g) Zu der behaupteten Rechtswidrigkeit "9. Unzulässige Kopie elektronischer Daten"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Im Übrigen ist darauf zu verweisen, dass der Wortlaut des Hausdurchsuchungsbefehls ausdrücklich die Sicherstellung von (physischen und) elektronischen Kopien anordnet und darin darauf hingewiesen wurde, dass auch nach Informationsquellen gesucht werden darf, die noch nicht bekannt sind. Die inhaltlich uneingeschränkte Kopie der gesamten Shares (Netzwerkverzeichnisse) mit der Bezeichnung ZN06-700 und ZN06-710 sowie die Kopie der gesamten Outlook-Postfächer der XXXX-Mitarbeiter /- XXXX, XXXX und XXXX stellen daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar.

Auch das Vorbringen der Beschwerdeführerinnen, wonach darüber hinaus die entsprechenden elektronischen Daten physisch nicht in den Geschäftsräumlichkeiten XXXX XXXX, gespeichert wären, die Kopie dieser Daten daher ein Abrufen vom zentralen Server in XXXX voraussetze und dies bedeute, dass die Hausdurchsuchung vom 19.08.2013 auch in räumlicher Hinsicht den Hausdurchsuchungsbefehl überschritten habe, da dieser ausdrücklich auf die Geschäftsräumlichkeiten XXXX XXXX, beschränkt sei, geht ins Leere. Denn die Beschwerdeführerinnen selbst verweisen durch Vorlage der gutachterlichen Stellungnahme von Professor Dr. XXXX vom 8.10.2013 zu Recht darauf, dass sich die Zugriffsrechte der belangten Behörde auf die geschäftlichen Unterlagen "unabhängig davon, in welcher Form sie vorliegen" beziehen: Auch elektronisch gespeicherte Unterlagen sind damit erfasst. Es kommt auch nicht darauf an, ob diese Unterlagen auf der Festplatte eines in den durchsuchten Räumlichkeiten befindlichen Endgeräts gespeichert werden oder ob diese Unterlagen auf externen Speicherplätzen (etwa dem zentralen Server in XXXX) liegen (vgl dazu auch Punkt 3.a)).

Eine offenkundige Überschreitung des richterlichen Befehls liegt diesbezüglich somit nicht vor.

3. h) Zu der behaupteten Rechtswidrigkeit "10. Unzulässige Weigerung, eine Versiegelung anzuerkennen"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Eine etwaige unzulässige Weigerung, eine Versiegelung anzuerkennen stellt daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar.

3. i) Zu der behaupteten Rechtswidrigkeit "11. Verbotener Einsatz einer Spionage-Software"

Hier ist auf die unter Punkt II.1. getroffenen Feststellungen zu verweisen. Diese können wie folgt zusammengefasst werden: Die belangte Behörde hat sich zur Umsetzung des durch den Hausdurchsuchungsbefehl vorgegebenen gerichtlichen Auftrages der Sicherstellung von (physischen und) elektronischen Kopien und um auch große Datenmengen schnell und effizient sichten zu können zweier IT-Experten des Bundeskriminalamtes (BKA) bedient.

Einem Experten des BKA ist in der Folge bei der Durchsuchung des Notebooks eines XXXX-Mitarbeiters aufgefallen, dass eine BITLOCKER-Verschlüsselung auf dem Notebook eingeschaltet war. Die Erstbeschwerdeführerin hat sich gegenüber dem Experten des BKA nicht kooperativ verhalten und das Administratorenpasswort nicht herausgegeben. Um zu verhindern, dass das BITLOCKER-Programm die Daten verschlüsselt und damit für die belangte Behörde unleserlich macht, haben die IT-Experten des BKA als Vorsichtsmaßnahme beschlossen, mit Hilfe des Einsatzes des forensischen Programms DumpIT den Arbeitsspeicher des durchsuchten Notebooks zu sichern, weil in diesem Arbeitsspeicher der Schlüssel für das kryptografische Programm BITLOCKER abgelegt ist. Ein IT-Experte des BKA hat in der Folge einen forensischen USB-Stick am Laptop des XXXX-Mitarbeiters angesteckt und vorerst nur versucht, das Programm DumpIT auszuführen. Die Ausführung des Programmes DumpIT hat jedoch aufgrund mangelnder Benutzerrechte nicht funktioniert. Das Programm hat sich nicht starten lassen. Die Ausführung des Programmes DumpIT ist somit fehlgeschlagen.

In der Folge wollten sich die IT-Experten des BKA einen Überblick über das Notebook verschaffen. Um diesen Überblick zu bekommen, wurde das Programm osTRIAGE verwendet. OsTRIAGE wird von ungefähr 50 Behörden weltweit eingesetzt. Dazu hat ein IT-Experte des BKA versucht, das Programm osTRIAGE vom USB-Stick aus zu starten, wobei das Programm auf dem Computer nicht installiert wurde. Der vorhandene Virenscanner hat beim Programm osTRIAGE angeschlagen. In der Folge ist das Programm nicht ordnungsgemäß gelaufen. Der IT-Experte des BKA hat daraufhin den Prozess osTRIAGE beendet.

Ein IT-Experte des BKA hat anschließend das auf dem Rechner befindliche Programm Snipping-Tool geöffnet und damit zu Dokumentationszwecken zwei Screenshots angefertigt. Weitere Handlungen haben die IT-Experten des BKA auf diesem Computer nicht durchgeführt. Auf dem Computer von Frau XXXX haben die IT-Experten des BKA keine forensische Software ausgeführt, sondern lediglich zu Dokumentationszwecken zwei Screenshots ebenfalls mit dem Programm Snipping-Tool angefertigt. Weitere Handlungen auf Computern der XXXX haben die IT-Experten des BKA nicht durchgeführt.

Wie unter Punkt 3.a) ausgeführt ist es zulässig, wenn die BWB bei einer Hausdurchsuchung geschäftliche Unterlagen sichtet, kopiert und Beweismittel in ihre Verfügungsmacht bringt, wenn sie dabei forensische Computerprogramme verwendet, um große Datenmengen schnell und effizient sichten zu können und um geschäftliche Unterlagen zu kopieren und diese in einer für sie lesbaren Form in ihre Verfügungsmacht zu bringen. Die BWB hat im gegenständlichen Fall lediglich vier Screenshots angefertigt und diese in ihre Verfügungsmacht gebracht. Alle anderen Versuche forensische Computerprogramme zu starten sind gescheitert. Eine offenkundige Überschreitung des richterlichen Befehls liegt daher diesbezüglich nicht vor.

3. j) Zu der behaupteten Rechtswidrigkeit "12. Verstöße gegen das Datenschutzgesetz"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Die gerügte Vorgangsweise der BWB stellt daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar. Zum gerügten "Einsatz einer Spionage-Software" wird auf Punkt 3.i) verwiesen.

Etwaige Verletzungen des DSG können vor der Datenschutzbehörde gerügt werden. Ein diesbezügliches Verfahren ist anhängig.

3. k) Zu der behaupteten Rechtswidrigkeit "13. Unterbliebene Zeugenbelehrungen"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Eine etwaige unterbliebene Zeugenbelehrung stellt daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar.

3. l) Zu der behaupteten Rechtswidrigkeit "14. Maßnahmenexzess in XXXX am 20.08.2013"

Zu diesem Vorbringen konnte die Ermittlung des Sachverhaltes unterbleiben, da selbst unter Zugrundelegung des Vorbringens der beschwerdeführenden Parteien auf die Judikatur des VwGH in seinem Erkenntnis vom 12. September 2013, Zl. 2013/04/0005, zu verweisen ist, wonach die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt nicht schon dadurch unterbrochen wird, dass im Vollzug des richterlichen Befehls Gesetzwidrigkeiten hinsichtlich der bei einem solchen Akt zu wahrenden Förmlichkeiten unterlaufen und die Modalitäten und die näheren Umstände, unter denen eine Hausdurchsuchung erfolgte, keine vor den unabhängigen Verwaltungssenaten - nunmehr dem Bundesverwaltungsgericht - selbständig bekämpfbaren Maßnahmen sind.

Eine etwaige ausschließliche Suche nach einem einzigen Dokument stellt daher jedenfalls keine offenkundige Überschreitung des richterlichen Befehls dar.

3. m) Zu den weiteren Anträgen

Die beantragte Vernehmung weiterer mehr als 20 Zeugen, die Unterbrechung des gegenständlichen Verfahrens sowie die Einholung eines Sachverständigengutachtens waren zur Ermittlung des entscheidungsrelevanten Sachverhaltes nicht notwendig.

3. n) Zusammenfassung

Zusammenfassend ergibt sich somit nach Durchführung einer mündlichen Verhandlung am 16.09.2014 und entsprechender rechtlicher Würdigung, dass bei der in der Zeit vom 19.08.2013 bis 20.08.2013 in XXXX, und am 20.08.2013 in XXXX, in den Geschäftsräumlichkeiten der erst- bis drittbeschwerdeführenden Parteien durchgeführten Hausdurchsuchung eine offenkundige Überschreitung des Hausdurchsuchungsbefehls des Oberlandesgerichts Wien vom 06.08.2013 erweitert mit Beschluss vom 20.08.2013 durch die BWB nicht stattgefunden hat und daher ein der Verwaltung zuzurechnendes Organhandeln nicht vorliegt. Die Maßnahmenbeschwerden waren daher zurückzuweisen.

B) Revision:

Gemäß § 25a Abs 1 VwGG hat das Verwaltungsgericht im Spruch seines Erkenntnisses oder Beschlusses auszusprechen, ob die Revision gemäß Art 133 Abs 4 B-VG zulässig ist. Der Ausspruch ist kurz zu begründen.

Die Revision ist gemäß Art 133 Abs. 4 B-VG nicht zulässig, weil die Entscheidung nicht von der Lösung einer Rechtsfrage abhängt, der grundsätzliche Bedeutung zukommt. Weder weicht die gegenständliche Entscheidung von der bisherigen Rechtsprechung des Verwaltungsgerichtshofes ab (VwGH 17.06.2014, 2012/04/0032), noch fehlt es an einer Rechtsprechung; weiters ist die vorliegende Rechtsprechung des Verwaltungsgerichtshofes auch nicht als uneinheitlich zu beurteilen. Auch liegen keine sonstigen Hinweise auf eine grundsätzliche Bedeutung der zu lösenden Rechtsfrage vor.

European Case Law Identifier

ECLI:AT:BVWG:2014:W134.2010888.1.00